Undurn the actions was	going to pass along a screen s s less impactful in November, so seeking out data prior and	heet freet theen has manth he	ovember and Decemi liperk ~2 million + PDI	er. It appears as is over their
(5)(B). (5)(D)				
· CC	PA 2011 1:53 PM ,(b)(7)(C) ste: It's worse than we know	***************************************		V
i will call in a moment.				
From (b)(6),(b)(7)(C) - Santt Friday, January 2	8, 2011 1:43 PM (b)(6),(b)(7)(C)	744WW.		-
TANKE CONTRACTOR OF THE PARTY O	It's worse than we know			
Speaking with (b)(8),(b)(c) currently underway and additional days of mass	just now about making sun discovering that the IP addre	e we have (7)(C) time as n sses associated with these sp	seded for the MIT evi ecific incidents have n	eluation umerous
ASAP if you think it usef for citrification, in light	to normalize against usual M that the individual responsibl ul and I le ^(b) know that I th of this information, it would a going forward. Certainly our to	e has already acquired the en ought you might be calling his earn that we need to try and o ack here merits some re-evals	tire JSTOR corpus. Gia n shortly after receiving understand the full plo pation, both concerning	d to have a call ig this message
the potential for additio	na) measures of prevention as	s we move forward. Also copy	ln(b)(8) at this june	g this case and cture.
nie weurinen lucideus	nal measures of prevention as	f we move forwerd. Also сору	$\log \ln \frac{(b)(6)}{a}$ at this jund	g this case and citure.
the potential for additio	nal measures of prevention a	i we move forwerd. Also copy	ing In <mark>(6)(6)</mark> at this jund	g this case and ciure.
the potential for addition (b)(6),(b)(7)(C) Thanks, b)(6),(b)(7)(C)	na) measures of prevention a	ғ we move forwerd. Also сору	ing In <u>i(b)(6</u> at this jund	g this case and ciure.
the potential for addition (b)(6),(b)(7)(C) Thanks,	na) measures of prevention a	ғ we move forwerd. Also сору	ing In <u>i(b)(6</u> at this jun	g this case and ciure.

Energy Control of the	Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
From Section 1	Monday, February 97, 2011 11:18 AM
Sent:	(b)(7)(C) BOS); External (b)(6),(b) ambridgepolice.org
2000 St	FW: MIT Undeter it's worse than we know
Subject	Las. Mit abaser ica mouse cum aus micha
(b)(6),(b)(7)	
From (C) [mailto	(6),(b)(7)(C) theka.org]
Sent: Friday, January 28, 2011	3:05 DM
To: Heymann, Stephen (USAMA	
Subject: FW: MIT Update: It's	venera than we know
Sampled (17) Par appearance	THE PARTY OF THE P
and this too.	
2/05/20/20/20/20	
(b)(6),(b)(7)	A COLUMN TO THE PARTY OF THE PA
Prom (C)	
Sonta Pricing, January 28, 2011	3502 PM
Te: (b)(6),(b)(7)(C)	
(b)(6),(b)(7)(C)	 .
Subject: RE: MIT Update: It's	vorse than we know
WAY A	
I do know from (b)(7)/ initial a	nalysis that the downloading was done systematically using sequential increases in our
stable URLs. That is, get stable	JRL 12345, get stable URL 12346, 12347, 12348 and so on.
This talks are a four things. Con. t	hat the previous activity was similar to the pattern(b) is seeing. That is, not targeted
the case of the transferre	dence to an entire corpus grab approach. Don't care what it is I am getting, just get me
	marine to an autrite corber Rom objectory pair cone same at the gas Barting bot factors
the next one.	
D)(6).	
(7)(g	
(b)(6),(b)(7)(C)	
Prom:	
Sent: Friday, January 29, 2011	2:50 PM
To	
(b)(6),(b)(7)(
Subject: Re: MIT Update: It's v	verse than we lurew
•	
This doesn't appear to be targete	d towards research articles or any particular titles, collections, or disciplines. For the 2.8
million in Nov and Dec, the break	down by article type is:
Research articles - 1,385,569	
Raviaws - 938,063	
Misc - 459,457	
Misc - 459,457 News - 62,127	
Misc - 459,457	
Misc = 459,457 News = 62,127 Editorial = 9,472	tists to the corous as a whole. I'd say the he was oning after averything.
Misc = 459,457 News = 62,127 Editorial = 9,472	elate to the corpus as a whole. I'd say the he was going after everything.
Misc - 459,457 News - 62,127 Editorial - 9,472 Those numbers more or less corr	
Misc = 459,457 News = 62,127 Editorial = 9,472 Those numbers more or less com- From (b)(6),(b)(7)(C)	Pithaka.org>
Misc - 459,457 News - 62,127 Editorial - 9,472 Those numbers more or less corr	Pithaka.om>

	(b)(6),(b)(7)(C)						
Ce		b					
30	eject: Re: MIT Upd	ste: it's wors	e than we know	W			12
Att	ached are 2 screen	shots donieti	u PDF daumles	el articipe from i	All the Marmarker	and Basember -	no aboudo c ^M
901	whicads and totals :	2.854,824 for	the 2 months. "	The other filters	nii tur teovember: cut downloads fra	and December, Qi Im the 2 iP's that i	ne snows all ook to be associated
WIL	n una gowniogg adi	1 36 KBX(6)*(6)	(1)(0)		nd totals 17 BEE fo	othe 2 month ass	ted Secondalization
501	ne legitimete down	ooks may have	re occurred yron	in the 3 Whereast	De le carriel attil lu	ands to one that a	house 2 0 military illean
U	MINDERS ODCINING G	HTE NOVERS	ier and Decemb	Mr. We know ti	at come illered des	unbarline company	d malar as Maranahan
217	i bing teuritiak' i 66i	T REVE LIQUE	: Numbers vet.	Rist Inching at 41	a amph wan see as	معددت محصم فمناه ها	
aft	ine. It wouldn't be	much of a ch	at weak or Dec	(over 100k.ggy)	it seems nitely thi	s extended into Ja	nnery for some period
24.48	e en a contribilistratific	MI WIS CIEIT.	I CODECT TO NAV	e stab vigural 9	vallable for routew	to Monday 196 at	may have occurred
and	Sept numbers as w	reli to comple	te the picture.			of monay, the	to seem meening occ
(b)(6),						
(b)(7	70						
TITIS Em	(b)(8),(b)(7)(C)				***	*****	····
Fro	e: Fri, 28 Jan 2011	4442.59 ne	ithaka.org	•			
Tel(b)(8),(b)(7)(C)		aka.om>				
Cd	b)(6),(b)(7)(C)	int	ratra orgo (b)(6)	,(b)(7)(C)	Ithalia.org		
Sul	OCE RE: MIT Upda	te: It's worse	than we know		DURINGOIS		
30,	with September an	d October, w	hat does the n	ıumber look ilki	7 Still looking like	the entire corpu	15 ?
	~ (b)(6),(b)(7) —		~ ^			19 10 to 10	
	M(C) 2: Friday, January	10 2014 2.41	. 684				
TO			३ स्थाप 				
œ)(8),(b)(7)(C)					
Sub	oct: RE: MIT Upd	ete: It's wors	e than we know	W			
)(8) ,	(b)(7)						
1							
Still (digging and (b)	Roine to ose	alone a ermen	t chot of what t	o la applica for Star		mber. It appears as
thou	gh the activity was	iess impacti	ul in November	r. but lust these	e is seeing for No	vernoer and Dece	mber, it appears as
nam	nal usage (b) s al	so seeking ou	it data prior en	id since for revi	tw.	MERK & INTERNITY (LOL2 CASE TUBIL
7					-		6
).							
lann	(b)(6),(b)(7)(C)			-# . A.M		~	
i wii kani	t Fiday, January 2	<u> 2011 1153</u>	064				····
les.	(b)(8),(b)(7)(F-	FPI				583
)CI							
	int RE: MIT Upda	te: It's worse	than we know	1		•	
. القين	call in a moment.						
wa.							
	(b)(6),(b)(7)	*/4*******	Mr. 1		.t	······································	
	Friday, January 26	3. 2011 142	DM	,		•	
4		6),(b)(7)(C)	re d				
9_						•	
	Ch Pir Update: h	's worse ther	we know				

	(b)(a),(b)(7)(C)	
Prom:		cambridgepolice.org>
Sent:	Wednesday, February 02, 2	011 837 AM
Tec	Heymann, Stephen (USAM)	
Subjects	RE: MIT Update: It's worse t	
	The transfer of the same of th	the same of the sa
Got it		
GOT II		
· · · · · · · · · · · · · · · · · · ·	(b)(8),(b)(7)(C)	
Premi Heymann, Stephen (USA)		usdoj.gov]
Sent: Wednesday, February 02,	2011 8:32 AM	
Te:(b)(6).(b)(7)(C) (BOS);(6)(6),(b)(7)(C)	
Subjects FW: MIT Update: It's v	vorse thein we know	
		8
From: (b)(6),(b)(7) [malto (b)	(8),(b)(7)(C)	
Sent: Friday, January 28, 2011		
To: Heymann, Stephen (USAMA)		
Subject: FW: MIT Update: It's v	orse then we know	
	, , , , , , , , , , , , , , , , , , , ,	
and this too.		
(b)(6),(b)(7)		
Proms(C)		
Sont: Edday, January 28, 2011 3	1:02 PM	
Tel (b)(6),(b)(7)(C)	T	
Cc (D)(B),(D)(7)(ත්	
Subject: RE: MIT Update: It's w		
(b)(d),		
I do know from (b)(7)(C linitial an	alusis that the downloading	was done systematically using sequential increases in our
stable URLs. That is, not stable U		
This talle are a few things One th	at the medians activity was	similar to the patiern(6) is seeing. That is, not targeted
towards times Two It leads recei	page to an author course or	ib epproach. Don't care what it is I am getting, just put me
the next one.	serios do am entido corpus gra	in abbinocur non r cus auste it at t au Barrust lest Bar us
the next one.		
(6) (6) (6) (7)		
(0). (h)/7		
WOMEN GOVERNORS		
Promis		
Sent: Friday, January 28, 2011 2	:50 PM	
To-(h)(h)(h)(z)(c)		
Cc (b)(6),(b)(7)(C		
Subjects Re: MLT Update: It's w	tree than we know	
This descrit senses to be formeded	tomande managenh antitue on	any particular titles, collections, or disciplines. For the 2.8
million in Nov and Dec, the breakd		only has notice armin attractional of appropriate Let #14 916
mimon in Nov and Dec, the breisid Research articles — 1,385,569	nam od energe zábe re:	
Reviews - 938,063		
Misc - 459,457		
News - 62,127		
California _ 6 477		

-		(b)(6),(b)(7)(C)		
From:	leymann, Stephen (USAMA	(b)(0),(b)(7)(C)	Dusdoj.gov>	
Sent:	Wednesday, February 02, 2	011 8:32 AM		
To: (b)(6),(b)	. , , , ,	771/21	cambridgepolice.org	
Subject:	FW: MIT Update: It's worse	than we know		
/b/6\/b/7\/C\	And the second second	Walter	.a. al. 1511114, 81125 personana anna 4 14 anna anna 14	lang scores at 41 fgs. gg. common man
From: (b)(6),(b)(7)(C) mailto (b)(6)),(b)(7)(C) pithaka.org]			
Sent: Friday, January 28, 2011 3:0)5 PM			
To: Heymann, Stephen (USAMA)				
Subject: FW: MIT Update: It's wo	rse than we know			
and this too.				
/b/G//b//7\	*** * *** * ##########################		175 7/6-13, 434513322 becover a necession amount a contra	and the same of th
(b)(6),(b)(7)				
Sent: Friday, January 28, 2011 3:0	<u> 32</u> PM			
To:				
(b)(6),(b)(7)(C				
Subject: RE: MIT Update: It's wo	ise than we know			
(b)(6),	e. Name akan kakin dan ingkalan dan k		aatiaalla urinn ennunn	tial increases in our
i do know from (b)(7)(C initial ana	lysis that the downloading	was done system	usticativ natification	fill lithingsca in oa
stable URLs. That is, get stable UR	L 12345, get stable UKL 12	346, 1234/, 1234	is and so on.	
			(b)	
This tells us a few things. One, tha	t the previous activity was	similar to the pai	ttern(6).() is seeing. In	lat is, not targeted
towards types. Two, it lends crede	nce to an entire corpus gr	ab approach. Don	n't care what it is i am	Betriug' Inot Ber ille
the next one.	ti.			
En CAS				
(b)(6), (b)(7)(
(b)(6),(b)(7)(C)	ALA MIN WAS IN A ST TO THE			
From	311 C C C C C C C C C C C C C C C C C C			
Sent: Friday, January 28, 2011 2:	50 PM			
To:				
Cc: (b)(6),(b)(7)(C)				
Subject: Re: MIT Update: It's wo	rse than we know			
		to	to a continue to one official	Man English 25
This doesn't appear to be targeted t	owards research articles or	any particular title	es, collections, or disci	annes. For the 4.0
million in Nov and Dec, the breakdo	wn by article type is:			
Research articles - 1,385,569				
Reviews - 938,063			•	
Misc 459,457				
News - 62,127				
Editorial — 9,472				
Those numbers more or less correla	ite to the corpus as a whole	. I'd say the he wa	as going after everythin	9 5.
(b)(6),(b)(7)(C)	tak also a ma	and the section of th	FFE days with adolated to bear from common in our section (i.e. on all to the even	
Promi	ithaka.org>			•
Date: Fri, 28 Jan 2011 14:28:43 -05		C)	Males area	
To (b)(6),(b)(7)(C)	Ithaka.org>	9	ithaka.org>	

(6)(8),(6)(7)(C)	Luka ann			
Cer	and a decide	thaka.one			
Subjects Re: I	AIT Update: It's wi	orse than we linow			
			4 - 24-7 - 44		
Atteshed are	ž screen ehots depi	citing PDF download activity	trom MIT for N	avamber and Decemb	er. One shows all
dewnloads en	d totain 2,654,824	for the 2 months. The other	filters out don	mineds from the 3 IPs	that book to be associated
with the down	nlead abuse (b)(6),	(B)(7)(C)	land totals	17,865 for the 2 man	in period. Recognizing that
some legitims	to downloads may	have occurred from the 3 fi	litered IP's, it we	suld still be safe to say	that about 2.8 million Higgs
downlands oc	wolf gafrub borrug	imberend December. We l	mow that come	illugal downloading o	curred prior to November
end into Janu	my. I don't have th	iosa numbers yet. Det lookl	ng at the graph	you can see that some	pretty negrepsive
downloading	was taking place th	e last week of Dec (over 10	Dh.day), Asson	w likely this extended	into January for some period
of time. It we	uldn't be much of	n stretch to any that as much	h of a million or	more additional down	lands may have occurred
that are not n	effected on this chi	ert. I ampact to have January	data avalleble	for review by Monday	I'll also start fooding Oct
	bers as well to con			San Hay Massacraw	
(b)(0),					
EXT					
	12.073				
(p)(e),((5)(7)(C)	- Pro- Warmen	######################################		
From		Dithaka.cop			
Duhnt Frl. 28	Inn 2011 14:13:57	_0500			
To (6)(8),(b)(7)(C)	Ithalm.on ((b)(0),(b)(7)(PA .	ı	
Co		Rhaka.ons	6)	Ithalos.ons>	
	Vir Undaha: IVs W	ores than we lanow			
So with Sont	omher and Ortob	er, what does the number	look like? Still	looking like the entire	corpus?
CARDINAGO		my series about mon transcript			
(b)(d),((5)(7)(C)]	the state of the s		M.M	
From	1916	E9			
	January 28, 2013	. <u>2:1</u> 0 PM			
Te	b)(8),(b)(7)(C)	ì			
(08					
Subject: RE	: MIT Update: It's	worse than we know			
(b)(8),(b)					
(7)(C)					
	751				
Still digging o	indical a going to	pass along a screen shot o	of what he is se	eing for November at	nd December. It appears as
though the a	ethilite was less im	pactful in November, but j	ust these two s	nonths beliperk "2 m	illion + PDFs over their
		ng out data prior and since		tri	
(1041) and	W.C.				
(D)(0),				19	
() (). () () ()					
- 75VA	(b)(7)(C)		h/////		
CTORIN					
Conta Priday	, January 28, 2011	1:53 P04			
Te: Ce:	(p)(g)'(p)	men			
Cet					
Subject RE	: MIT Update: The	worse than we know			
I will call in o	moment.				
(b)(0)	(b)(7)	, d			
(C)	January 28, 2011	1402 800			8
		2003		2. 1	*
Tot	(b)(a),(b)(7)((C)			
UC)	T Undate: It's wor	8		¥	
II SERVICE OF THE PARTY OF THE					

BEGIN PGP SIGNATURE D(0).(0)(7)(C)	8

Proms	(b)(d),(b)(7)(C)	
Sent	@cambridgepotice.org>	
Te:	(b)(6),(b)(7)(C) BOS) (b)(6),(b)(7)	
Subject	RE: Follow-up questions with (C)	
CC (b)(6),(b) Subject RE: Follow-	(BOS) [mailto] usss.dhs.gov] usss.dhs.gov] (7)(C) (b)(6),(b)(7)	
(b)(6),(b)(7)(C) Proma (b)(6),(b)(7)(C) Sept: Monday, Januar Tol(b)(6),(b)(7)(C) Ce Subject: Re: Follow-u	(BOS); Edema (b)(6),(b) cambridgepolice.org; (b)(6),(b)(7)(C)	gov
open all day, with on b)(8), b)(7)(time I've got available on Wednesday is after 4:00pm, due to an all-defined like that might not work for Steve, but if it does, it works for me, ally a hard-stop for me at 5:30pm. Friday also has me tied up 9am-3pm, does 3:00pm work for you to meet down in the state of the stat	Thursday is wide
cross one of moss).	furnish you with one of the duplicate drives that's already got the data	on it (or we can
here: (b)(8).(b)(7)(C) (b)(8). (b)(7)		
Hope all are well and	1 staying warm.	
Best, b)(d),(b)(7)(
b)(6),(b)(7)(C)	Analyst Services	
MPT (b)(8),(b)(7)(C)		2307

No.	(b)(8),(b)(7)(C)		
From:		·	MIT.EDU>	
Sent:	Monday.	January 24, 2011 :	10:15 PM	
To:	(b)(6),(b)(7)(C)	BOS); E	ternal (b)(6),(b)	idgepolice.org;
		Pusdojo	iov	
Cex			(b)(8),(b)(7)	
Subject:	Re: Follow	v-up questions wit	#(C)	(C)
				•
F31-3-4				
Steve (6). The	only time I've out availa	hle on Wednesd	ry is ofter 4:00mm, dia	to an all-day commitment
				orks for me. Thursday is wide
	th only a hard-stop for m			
5V6). 1	and a man mob the w	io in alcohor 11)(6).
b)(6), b)(7) for tome	mow. does 3:00nm work	for you to meet	down in (b) D Paris)(7) comment last meeting. I'm
thinking we can	inot fivelek was with an	a of the desirations	Appear that's alsowin	got the data on it (or we can
clane one of the	se). (5)(8). s located	e or an admica	a certaes cinics erreactà	Ros use debut out is for we can
100 (0)(0),(0)(1)(C	ee). Invent la rockled			
			,	
5)(8), b)(7)				
	II and storing many			
urobs mr ere we	ll and staying warm.			
.				
Beat,				
(6),(b)(7)				
<u>′ </u>				
(8),(b)(7)(C)				
	Security	Analyst		
IT Security Sys	ems & Services			
MIT				
	(b)(6),(b)(7)(C)			
	(b)(6),(b)(7)(C)	0.007		1
PGP Fingerprin	1-71-111-71-71-7			
				•
	((b)(6),(b)(7)(77		
On Jan 24, 2011		,	S) wrote:	
OH SELL 47, 201	, at o.es ray		s) wrote:	
Many annual de la				
MUSIC MOVING BE	good time for you to have	a conseignce cen	on wednesday?	
0100 18 th		100000		
AISO, IT IE WORKE IT	k Aor' i Monta kite to atab	by your office son	nationa tomorrow to go	t a copy of the packet data captur
	velilance file. When would	te a good time?		12
)(6)(6)(7)(C)				
(Carlo Company of the Carlo C				
U.S. Secret Service				
Boston Pield Office				
CANON CANON				
(b)(6),(b)(7)(C)		(b)(8),(b)(7)(C)		
	Scapinan (USAMA) [mailled		usdoj.gov]	
Bents Monday, Ji	THANY 24, 2011 5:45 PM			

On 10/12/10, the MIT Network and Information Security Team received an email from (b)(6),(b)(7)(C) stating that JSTOR informed her that excessive downloading came from IP address (b)(6),(b)(7)(C)
On 10/13/10, (C) traced the second occurrence of excessive unauthorized downloading to a computer registered on the network as "Grace Host" with an email of ghost420mailinator.com, a NAC address of 0017f22cb074 and computer name of "ghost-laptop", ((b)(6),(b)(7)) disabled
the host registrations identified as bogus. (b)(6),(b)(7)(C)
of Network Security and Support Services for MIT, notified (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) , the Director of MIT Operations and Infrastructure, that information indicated that the same unknown person appears to be using MIT guest registration from a wired connection in building 16.
On 11/29/10, the MIT Metwork and Information Security Team was notified by the MIT branch of the Institute of Electrical and Electronic Engineers that journal spidering has occurred on their site
and it was tracked to the Student Information Processing Board XVM cluster, a group of computers that are shared and that anyone in the
MIT community can use to host a Virtual Machine.
On 01/03/11, (C) received an email from (b)(6),(b)(7)(C) forwarded from (b)(6),(b)(7)(C) informing him that that the excessive downloading of journals
had begun again. $(b)(6),(b)(7)(C)$ On $01/04/11$, (C) emailed of Network
Operations, and (b)(6),(b)(7)(C) hit,edu) (b)(6) (b)(7)(C)
(b)(6),(b)(7)(C) for Network and Infrastructure Services for NIT, asking them to further pinpoint the location of the computer downloading the journals. At 0808,(b)(6),(b) located a computer hidden by a box connected to a switch in a wire closet in the basement of building 16. The computer was also connected to an external hard
drive. $(b)(8),(b)(7)$ established a packet capture of the same switch the computer was found attached to.
(b)(6),(b)(7) (C) also provided \$A (C) with a copy of historical network flow data concerning IP addresses (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) from 12/14/10 to
01/04/11 and DHCP log information for computers registered as ghost-
macbook and ghost-laptop. (b)(6),(b)(7) SA (C) contacted SA (C) (CID) at the CERT Coordination Center at
the Software Engineering Institute at Carnegie Mellon University. SA $(b)(6),(b)$ provided SA $(b)(6),(b)(7)$ with instructions to upload the data to the CERT drop box.
On 01/06/11, at approximately 1232, video surveillance showed the
individual later identified as Swartz return to the wire closet and remove the netbook and external hard drive. Later, (b)(0),(b)(7)(C) of the
MIT Police Department called (b)(6),(b)(7)(C) of the NIT Police Department
and stated that he had located the suspect later identified as Swartz riding his bicycle on Massachusetts Avenue near the intersection with Lee
Street in Cambridge, Massachusetts. (b)(6),(b)(7)(C) and SA (b)(6),(b)(7) 2339

Proces	(b)(d),(b)(7)(C)	
Sant	Tuesday, January 11, 2011 11:44 AM	
To:	Heymann, Stephen (USAMA)	
Ca	(b)(6),(b)(7)(C) (BOS); External (b)(6),(b)	sambridgepolice.org
Subject	RE: Confirming Interviews on Friday	
Yes (6),(b) is available	le. I should have made that clear in my earlier e-mail, but	was focused on identifying the right IS&T
(b)(6),(b)(7)(C)	7	
Office of the Gener		
	altute of Technology	
	Avenue, Building (0)(8),(0)	
Cambridge, MA 02 tel; (b)(6),(b)(7)(C)	139	
fax: 617-258-0267		
b)(6),(b) mlt.edu		W
	uttached documents contain information which may be confidential, sub	A
Intended recipient shall	materials are intended only for the use of the intended recipient. Delive I not compromise or waive such confidentiality, privilege, or exemption (b)(6),(b)(7)(C)	try of this message to eny person outer than yet
Tex (b)(8),(b)(7)(C) Cc:	Stephen (USAMA) [mailto] multip 11, 2011 10:06 AM (b)(6),(b)(7)(C) (BOS); Interviews on Friday	
		per EOUSA
	(b)(5),(b)(7)(C)	Parado
Steve:	8	
(b)(8),(b)(7)(Prose Sent: Tuesday, Jen To: Hermann, Steo Cc((b)(6),(b)(7)(C)	[mellio(b)(7)(MIT.EDU] wery 11, 2011 8:27 AM	
Suspect NE: Confi	ming Interviews on Fricey	

Steve -

Friday does work for us, although it might be easier to start at 11:00 (our conference room is booked from 9:30 to 11:00). Hopefully that's okay.

i have been in contact with the folks in IS&T and they came up with a slightly different list of names of people you'd probably want to speak with. They suggested $(b)(6)(b)(7)(C)$ and $(b)(6)(b)(7)$ (they've advised me that $(b)(6)$.
probably want to speak with. They suggested $(b)(6),(b)(7)(C)$ and $(b)(6),(b)(7)$ they've advised me that $(b)(8)$,
would likely be able to provide the same information that (b)(6),(b)(7)(C) and (b)(6),(b)(7) could provide). Also (b)(6),
(b)(6),(b)(7)(C) solvised me that he probably can't provide much information beyond what you could get from (b)(6),(b)(7)
(b)(6),(b)(7)(C) If you still want to speak to everyone, I'm sure we can make it work, but I just want to be su
we're being as afficient as possible. Let me know your thoughts.
We can hold the meeting in the Office of General Counsel conference room, located in room (6)(6)(6)(6)(1) get here, walk through the main entrance of 77 Massachusetts Avenue. You will enter a large lobby (known as Lobby 7) and see a lon corridor directly in front of you (known as the Infinite Corridor). Follow the Infinite Corridor until you enter another
large open lobby, known as Lobby 10 (you will see a large set of doors on the right that look out onto a large qued facts the Back Bay, called Killian Court). When you're in Lobby 10, there will be two elevators on your left (to further confus
things, you may see a sign that says "Lobby 13" with an arrow, but you're in Lobby 10 at that point). Take either of the elevators to the third floor. When you exit the elevators, immediately turn left and you will see a sign for the Office of
the General Counsel. Fellow the hallway until you see another sign for the entrance to the Office of the General
Counsel
I'm in meetings the bulk of today, so I will be somewhat inaccessible, but we can coordinate any additional details tomorrow.
(b)(8),(b)(7)(C)
Office of the General Counsel
Massachusetts institute of Technology
77 Messachusetts Avenue, Building (DKB)(DX7)
Cambridge, MA 02139
tel: (b)(6),(b)(7)(C)
farc 617-258-0267
(b)(8),(b)(7)(C)
This message and any attached documents contain information which may be confidential, subject to privilege, or exempt from disclosure under
appreciate New Tipers (Transfeld of the Internal of the Internal of Indiana, of the Internal o
intended rediptors shall not compromise or wake such confidentiality, privilege, or examplion from disclosure as to this communication.
(b)(6),(b)(7)(G)
Prome Heymann, Stephen (USAMA) [mailed
Santa Monday, January 10, 2011 4:30 PM
Tog(b)(e),(b)(7)(C) (b)(8),(b)(7)(C)
Oct BOS);
Subjects Confirming Interviews on Friday
(D)(D),(D)(7) (C)
Many and and bound from a second seco
If you can make it work from your end, let's do the interviews on Friday beginning at 10:00 a.m. I anticipate
(6)(6),(6),(7)(7) and (6)(8),(6)(7)(6) joining me. Tentatively, we would like to speak with the following five people in
the order listed (as well as anyone else you may think useful or appropriate).
(DRB)(DR7)(C)
e-remero ne-i

(b)(6),(b)(7)(C)	1			
Office of the Gene				
	titute of Technology			
		7		
: Cambridge, MA 0	Avenue, Building (0)(8),(0)(7)	J		
tel: (b)(6),(b)(7)(C			•	
fant: 617-258-026 b)(6),(b)(7) mit.edu				
applicable law. These	materials are intended only for the	a use of the intended recibles:	ntial, subject to privilings, or exempt from disci s. Delivery of this message to any person other emption from disclosure as to this communicat	than the
	(5)	(6),(b)(7)(C)	where the same state of the sa	
	Stephen (USANA) [melito	usdo).(gov]	
Tes (b)(8),(b)(7)(C	10, 2011 4:30 PM (b)(8),(b)(7)(C)	-		
Cal	(BOS);		•	
	ng Interviews on Friday			
	A Tring Aides OIL LINEA			
(0)(0).(0)				
If you can make I	t work from your and, let	s do the intendeus on	Friday beginning at 10:00 a.m. I an	ticinata.
(b)(6),(b)(7)(C) and (b)	8)/b)//(C) inline me Te	statuch un mand il	te to speak with the following five p	oupate
the order listed (as well as anyone else you	mourely, we would no a	re to shedy and mis tologous in the	achia in
-in as man shoot a	ns seen as enfond one loc	साम्रे सामाप्र एक्समा का व्य	ppoprietej.	
(D)(8),(B)(7)(C)				
	i		•	
			EFOUGA	
			per EOUSA	
1				
			•	
	1			
1				
(0)(0)(0)(0)				
	€2			

Thank you, Steve

<u> </u>	(b)(6),(b)(7)(C)
From:	IT.EDU>
Sent	Tuccdoy, January 11, 2011 8:27 AM
To:	(b)(6),(b)(7)(C) BOS); External (C)(6),(b) cambridgepolice.org
Ce	(b)(8),(b)(7)(C) BOS); External((b)(8),(b) cambridgepolice.org
Subjest	RE: Confirming Interviews on Friday
Stave -	
Friday does work f 11:00). Hopefully	or us, although it might be easier to start at 11:00 (our conference room is booked from 9:30 to that's citay.
probably want to s would likely be abl 8),(b)(7)(C) advised 8),(b)(7)(C)	peak with the folks in IS&T and they came up with a slightly different list of names of people you'd peak with. They suggested $(b)(6),(b)(7)(C)$ and $(b)(6),(b)(7)$ hey've advised me that $(b)(6)$ and $(b)(6),(b)(7)$ bould provide). Also $(b)(6)$ me that he probably cen't provide much information beyond what you could get from $(b)(6),(b)(7)$. If you still want to speak to everyone, i'm sure we can make it work, but i just want to be cleant as possible. Let me know your thoughts.
through the main corridor directly in large open jobby, i	peeting in the Office of General Counsel conference room, located in room ((10,0)) To get here, we entrunce of 77 Messachusetts Avenue. You will enter a large lobby (known as Lobby 7) and see a known of you (known as the infinite Corridor). Follow the infinite Corridor until you enter another known as Lobby 10 (you will use a large set of doors on the right that look out onto a large quad fact (to further conference). When you're in Lobby 10, there will be two elevators on your left (to further conference).
elevators to the th	e a sign that says "Lobby 13" with an arrow, but you're in Lobby 10 at that point). Take either of the floor. When you exit the elevators, immediately turn left and you will see a sign for the Office of the General el. Follow the hellway until you see another sign for the entrance to the Office of the General
elevators to the th the General Couns Counsel.	e a sign that says "Lobby 13" with an arrow, but you're in Lobby 10 at that point). Take either of ti ird floor. When you exit the elevators, immediately turn left and you will see a sign for the Office (
elevators to the th the General Couns Counsel. I'm in meetings the tomorrow. (6),	e a sign that says "Lobby 13" with an arrow, but you're in Lobby 10 at that point). Take either of the floor. When you exit the elevators, immediately turn left and you will see a sign for the Office of the General el. Follow the hellway until you see another sign for the entrance to the Office of the General
elevators to the th the General Course Counsel. I'm in meetings the tomorrow. (6),(6), (6),(b)(7)(C)	e a sign that says "Lobby 23" with an arrow, but you're in Lobby 30 at that point). Take either of the floor. When you exit the elevators, immediately turn left and you will see a sign for the Office of the General el. Follow the hellway until you see another sign for the entrance to the Office of the General bulk of today, so I will be somewhat inaccessible, but we can coordinate any additional datalis
elevators to the the General Counsel. I'm in meetings the tomorrow. (6),(6), (6),(b)(7)(C) Office of the General Counsel.	e a sign that says "Lobby 23" with an arrow, but you're in Lobby 30 at that point). Take either of the floor. When you exit the elevators, immediately turn left and you will see a sign for the Office of the General el. Follow the hallway until you see another sign for the entrance to the Office of the General bulk of today, so I will be somewhat inaccessible, but we can coordinate any additional details rai Counsel
elevators to the th the General Counse Counsel. I'm in meetings the tomorrow. (6),(6),(7)(C) Office of the Gene Massachusatts ins	e a sign that says "Lobby 23" with an arrow, but you're in Lobby 30 at that point). Take either of the floor. When you exit the elevators, immediately turn left and you will see a sign for the Office of the General el. Follow the hellway until you see another sign for the entrance to the Office of the General eluik of today, so I will be somewhat inaccessible, but we can coordinate any additional datalistic coursel citute of Technology
elevators to the the the General Course Counsel. I'm in meetings the tomorrow. (6),(6),(b)(7)(C) Office of the General Course	e a sign that says "Lobby 23" with an arrow, but you're in Lobby 30 at that point). Take either of the life floor. When you exit the elevators, immediately turn left and you will see a sign for the Office of the General el. Follow the hellway until you see another sign for the entrance to the Office of the General e bulk of today, so I will be sumawhat inaccessible, but we can coordinate any additional details rai Counsel titute of Technology Avenue, Building (0.00.007)
elevators to the the the General Course Counsel. I'm in meetings the tomorrow. (6),(6),(-)(7)(C) Office of the Gene Massachusatts instruments. Cambridge, MA Combridge, MA Combridge	e a sign that says "Lobby 23" with an arrow, but you're in Lobby 10 at that point). Take either of the life floor. When you exit the elevators, immediately turn left and you will see a sign for the Office of the General el. Follow the hellway until you see another sign for the entrance to the Office of the General e bulk of today, so I will be sumawhat inaccessible, but we can coordinate any additional details rai Counsel titute of Technology Avenue, Building (0)(0),(0)(7)
elevators to the the the General Course Counsel. I'm in meetings the tomorrow. (6),(6),(7)(C) Office of the Gene Massachusatts instruments. 77 Massachusatts instruments. Cambridge, MA Cottel:	e a sign that says "Lobby 13" with an arrow, but you're in Lobby 10 at that point). Take either of the floor. When you exit the elevators, immediately turn left and you will see a sign for the Office of the General el. Follow the hellway until you see another sign for the entrance to the Office of the General elevators, so I will be summediate inaccessible, but we can coordinate any additional details rel Counsel titute of Technology Avenue, Building (6)(8),(6)(7)(C)
elevators to the the the General Course Counsel. I'm in meetings the tomorrow. (6),(6),(-)(7)(C) Office of the Gene Massachusatts instruments. Cambridge, MA Combridge, MA Combridge	e a sign that says "Lobby 13" with an arrow, but you're in Lobby 10 at that point). Take either of the floor. When you exit the elevators, immediately turn left and you will see a sign for the Office of the General el. Follow the hellway until you see another sign for the entrance to the Office of the General elevators, so I will be summediate inaccessible, but we can coordinate any additional details rel Counsel titute of Technology Avenue, Building (6)(8),(6)(7)(C)
elevators to the the the General Course. I'm in meetings the tomorrow. (6),(b),(7)(C) Office of the Gene Massachusatts instruments. Cambridge, MA Cotel: fax: 617-258-0267 (b),(b)(7) mit.edu This message and any applicable law. These intended recipient shall	e a sign that says "Lobby 13" with an arrow, but you're in Lobby 10 at that point). Take either of the floor. When you end the elevators, immediately turn left and you will see a sign for the Office of the General el. Follow the hallway until you see another sign for the entrance to the Office of the General elevators in the hallway until you see another sign for the entrance to the Office of the General elevators in the hallway until you see another sign for the entrance to the Office of the General elevators in the hall was a sign for the General elevators in the conditional districts of today, so I will be somewhat inaccessible, but we can coordinate any additional districts of Technology Aversus, Building (p)(8),(b)(7)(C)) Ittacked documents contain information which may be confidential, subject to privilege, or exampt from disclasure understates are intended only for the use of the intended recipient. Delivery of this message to any person other than the instruction are seven to this communication.
elevators to the the the General Course. I'm in meetings the tomorrow. (6),(b),(7)(C) Office of the Gene Massachusatts instruments. Cambridge, MA Cotel: fax: 617-258-0267 (b),(b)(7) mit.edu This message and any applicable law. These intended recipient shall	e a sign that says "Lobby 1.3" with an arrow, but you're in Lobby 10 at that point). Take either of the front of the floor. When you exit the elevators, immediately turn left and you will see a sign for the Office of the Congress. Follow the hallway until you see another sign for the entrance to the Office of the General abulk of today, so I will be summinate inaccessible, but we can coordinate any additional datells are consolidated by the confidential, subject to privilege, or estimate from discionare under naturals are intended only for the use of the intended recision. Delivery of this message to any person other than the

Comparison Com	On 09/27/10 at approximately 1028, the MIT Network and Information Security Team
Solution	receives an email from (b)(6),(b)(7)(C) the MIT (b)(6),(b)(7)(C)
identified IP addresses. [DNS.DIT/C] Biourity Analyst discovers natwork registration for "Gary Most" used small address ghost-machock" register on the network on 09/24/10. [DNS.DIT/C] Not" used small address ghost-machock" register on the network on 09/24/10. [DNS.DIT/C] On 10/22/10 at approximately 1115 [DNS.DIT/C] emails[DNS.DIT/C] the MITONO.DIT/C] the MITONO.DIT/C] from JSTOR Operations Staff candidated the computer registration. On 10/22/10, the MIT Network and Information Security Team received an email from [DNS.DIT/C] traced that JSTOR had been cut off again due to excessive downloading came from IP address [DNS.DIT/C]. On 10/22/10, the MIT Network and Information Security Team received an email from [DNS.DIT/C] traced the second cogurrence of excessive masuborized downloading to a computer registered on the network as "Grace Host" with an email of ghost-talemail instor. com, a MAC address of 001722cb074 and computer mass of "ghost-talemail instor. com, a MAC address of 001722cb074 and computer mass of "ghost-talemail instor. com, a MAC address of 001722cb074 and computer mass of "ghost-talemail instor. com, a MAC address of 001722cb074 and computer mass of "ghost-talemail instor. com, a MAC address of 001722cb074 and computer mass of "ghost-talemail instor. com, a MAC address of 001722cb074 and computer mass of "ghost-talemail instor. com, a MAC address of 001722cb074 and computer mass of "ghost-talemail instor. com, a MAC address of 001722cb074 and computer mass of "ghost-talemail instor. com, a MAC address of 001722cb074 and computer mass of "ghost-talemail instor. com, a MAC address of 001722cb074 and computer mass of "ghost-talemail instor. com, and the mass of 001722cb07/C] [DNS.DIT/C]	WAY AND THE SAME TO THE SAME TO THE PROPERTY OF THE PROPERTY O
Rost wed email address ghost-machock* register on the network registration for 'dary Rost' wed email address ghost-machock* register on the network on 09/24/10. (b/6),(b/7)(C)	1 dent 1 51 A 1 A 1 A 1 A 1 A 1 A 1 A 1 A 1 A
Host" used email address ghost-machod: register on the network on 09/24/10. [b](6)(b)(7)(C) classed name ophost-machod: register on the network on 09/24/10. [b](6)(b)(7)(C) classed name of the Name	Whys/Wyyc: security Analyst discovers network registration for 'Gary
On 10/09/10 at approximately 1115 (b)(0)(b)(7)(C) trom JETCR Operations Staff emails[b)(0)(b)(7)(C) the MIT(b)(0)(b)(7)(C) to inform her that MIT's access to JETCR had been out off again due to excessive downloading. On 10/13/10, the MIT Metwork and Information Security Team received an email from [b)(0)(b)(7)(C) latating that JETCR had told her the excessive downloading came from IP address [b)(0)(b)(7)(C) On 10/13/10, [b)(5)(b)(7)(C) On 10/13/10, [b)(5)(b)(1)(C) On 10/13/10, [b)(5)(b)(1)(C) On 10/13/10, [b)(5)(b)(1)(C) On 10/13/10, [b)(5)(b)(7)(C) Interpretation of the new months are accessive unauthorised downloading to a computer registered on the network as "Grace Rost" with an email of ghost428mailinator, con, a MAC address of 0017522ab074 and computer name of "ghost-1aptop", [b)(5)(b)(7)(C) Interpretation of the host registration independent of the computer name of "ghost-1aptop", [b)(5)(b)(7)(C) Interpretation of [b)(5)(b)(7)(C) Interpretation of [b)(5)(b)(7)(C) Interpretation indicates that the same unknown person appears to be using MIT guest registration from a wired connection in building 14. On 11/29/10, the MIT Metwork and Information Security Team is notified by the MIT branch of the Institute of Electrical and Electronic Engineers that journal spidering is cocurring on their size and it is tracked to the student Information Processing Board XVM cluster, a group of computers that are shared and that anyons in the MIT community can host a virtual Mechine on. On 11/20/10, the Virtual Machine downloading journals from JETCR is taken offline. On 01/03/11 at approximately 0249, [b)(6)(b)(7)(c) matted from [b)(6)(b)(7)(c) man(b)(6)(b)(7)(c) man(b)(6)(6)(7)(c) man(b)(6)(6)(6)(7)(c) man(b)(6)	Heat" used email address chost@mailinator.com, a MAC address of 00235a735ffb and
On 10/19/10 at approximately 1115 [0](0](0)(0)(1)(C)	computer name "ghost-macbook" register on the network on 09/24/10. (D)(B)(D)(/)(C)
to JSTOR had been cut off again due to excessive downloading. On 10/12/10, the MIT Metwork and Information Security Team received an email from [D(S),D(T)C] stating that JSTOR had told her the excessive downloading came from IP address [D(S),D(T)C] traced the second cocurrence of excessive unauthorized downloading to a computer registered on the network as "drace Host" with an email of ghost-laptop", [D(S),D(T)C] traced the second cocurrence of excessive unauthorized downloading to a computer registered on the network as "drace Host" with an email of ghost-laptop", [D(S),D(T)C] traced the host registrations identified as longus. [D(S),D(T)C] traced the host registrations identified as for NIT motified [D(S),D(T)C] traced the host registrations identified as for NIT motified [D(S),D(T)C] traced the host registrations identified as for NIT motified [D(S),D(T)C] traced to host registrations and information indexics that the same unknown person appears to be using MIT guest registration from a wired connection in building 16. On 11/29/10, the MIT Metwork and Information Security Team is notified by the MIT hranch of the Institute of Electrical and Electronic Engineers that journal spidering is cocurring on their site and it is tracked to the Student Information Processing Board XVM cluster, a group of computers that are shared and that anyons in the MIT community can host a virtual Machine on. On 11/29/10, the Virtual Machine downloading journals from JSTOR is taken offline. On 01/03/11 at approximately 1440, [D(S),D(T)] received an email from [D(S),D(T)(C)] and [D(S),D(T)(C)] the MIT seems of the Normal State of the MIT general State of the State of the Computer downloading the journals. At 0808 [D(S),D(T)(C)] the MIT seems of building 16. D(S),D(D(T)(C) and (D(S),D(T)(C) and (D(
to JSTOR had been cut off again due to excessive downloading. On 10/12/10, the MIT Metwork and Information Security Team received an email from [D(S),D(T)C] stating that JSTOR had told her the excessive downloading came from IP address [D(S),D(T)C] traced the second cocurrence of excessive unauthorized downloading to a computer registered on the network as "drace Host" with an email of ghost-laptop", [D(S),D(T)C] traced the second cocurrence of excessive unauthorized downloading to a computer registered on the network as "drace Host" with an email of ghost-laptop", [D(S),D(T)C] traced the host registrations identified as longus. [D(S),D(T)C] traced the host registrations identified as for NIT motified [D(S),D(T)C] traced the host registrations identified as for NIT motified [D(S),D(T)C] traced the host registrations identified as for NIT motified [D(S),D(T)C] traced to host registrations and information indexics that the same unknown person appears to be using MIT guest registration from a wired connection in building 16. On 11/29/10, the MIT Metwork and Information Security Team is notified by the MIT hranch of the Institute of Electrical and Electronic Engineers that journal spidering is cocurring on their site and it is tracked to the Student Information Processing Board XVM cluster, a group of computers that are shared and that anyons in the MIT community can host a virtual Machine on. On 11/29/10, the Virtual Machine downloading journals from JSTOR is taken offline. On 01/03/11 at approximately 1440, [D(S),D(T)] received an email from [D(S),D(T)(C)] and [D(S),D(T)(C)] the MIT seems of the Normal State of the MIT general State of the State of the Computer downloading the journals. At 0808 [D(S),D(T)(C)] the MIT seems of building 16. D(S),D(D(T)(C) and (D(S),D(T)(C) and (D(On 10/00/10 at approximately 1115 (b)(6),(b)(7)(C) From JETOR Contrations Staff
to JSTOR had been cut off again due to excessive downloading. On 10/12/10, the MIT Metwork and Information Security Team received an email from [008],(b)(7/C) stating that JSTOR had told her the excessive downloading came from IP address [008],(b)(7/C) on 10/13/10, D(00/D) traced the second occurrence of excessive unauthorized downloading to a computer registered on the network as "Grace Host" with an email of ghostd2mmail.nator.com, a MAC address of 001722cb074 and computer meas of "ghost-laptop", [00/0,0] disabled the hoet registrations identified as bogus. [00/0,0](7/C) Menager of [0](8),007/C) MIT Operations identified as bogus. [00/0,0](0)(7/C) Menager of [0](8),007/C) MIT Operations identified as bogus. [00/0,0](7/C) MIT operation indicates that the same unknown person appears to be using MIT guest registration from a wired connection in building 16. On 11/29/10, the MIT Metwork and Information Security Team is notified by the MIT branch of the Institute of Electrical and Electronic Engineers that journal spidering is occurring on their site and it is tracked to the Student Information Processing Seard XVM cluster, a group of computers that are shared and that anyone in the MIT community can host a Virtual Machine on. On 11/20/10, the Virtual Machine downloading journals from JSTOR is taken offline. On 01/03/11 at approximately 1440, [00/0,00/7/C] received an email from forwarded from [00/0,00/7/C] MIT Operation of the computer downloading the journals and a menal from the MIT community of the MIT setting the total income and [00/0,00/7/C] MIT Operation of the computer downloading the journals. At 0000 [00/0,00/7/C] D(00/0,00/7/C) MIT Operation of the computer downloading the journals. At 0000 [00/0,00/7/C] MIT Operation of the computer downloading the journals. At 0000 [00/0,00/7/C] D(00/0,00/7/C) MIT Operation of the computer downloading the journals. At 0000 [00/0,00/7/C] D(00/0,00/7/C) MIT Operation of the computer is also commerced to an external hard drive.	emails $(b)(6), (b)(7)(C)$ the MIT(b)(6),(b)(7)(C) to inform her that MIT's access
address [0.(6),(0)(7)(C) address [0.(6),(0)(T)(C) On 10/13/10, [0.(6),(6)] traced the second occurrence of excessive unauthorized downloading to a computer registered on the natwork as "Grace Host" with an email of ghost428mailinator com, a MAC address of 0017f22cb074 and computer name of "ghost-laptor" [0.(6),(6)) disabled the host registrations identified as for NIT motifies [0.(6),(6),(7)(C)] Ind [0.(6),	to JSTOR had been cut off again due to excessive downloading.
address [0.(6),(0)(7)(C) address [0.(6),(0)(T)(C) On 10/13/10, [0.(6),(6)] traced the second occurrence of excessive unauthorized downloading to a computer registered on the natwork as "Grace Host" with an email of ghost428mailinator com, a MAC address of 0017f22cb074 and computer name of "ghost-laptor" [0.(6),(6)) disabled the host registrations identified as for NIT motifies [0.(6),(6),(7)(C)] Ind [0.(6),	
on 10/13/10, [Di(6),(b)] traced the second occurrance of excessive unauthorized downloading to a computer registered on the network as "Grace Host" with an email of ghost-lemnitinator.com, a MAC address of 01/12/20/074 and computer name of "ghost-lantop". [Di(6),(b)] disabled the host registrations identified as hogus. [Di(6),(b),(f)(C)] has [Di(6),(b),(f)(C)] MIT Operations and Infrastrocture that information indicates that the same unknown person appears to be using MIT guest registration from a wired connection in building by the MIT hranch of the Institute of Electrical and Electronic Engineers that journal spidering is cocurring on their site and it is tracked to the Student Information Processing Board XVM cluster, a group of computers that are shared and that anyone in the MIT community can host a virtual Machine on. On 11/20/10, the Virtual Machine downloading journals from JSTOR is taken offline. On 01/03/11 at approximately 1440, [Di(6),(b)/7)C] received an email from JSTOR is taken offline. On 01/03/11 at approximately 1440, [Di(6),(b)/7)C] received an email from JSTOR is taken offline. On 01/04/11 at approximately 0242, [Di(6),(b)/7)C] received an email from [Di(6),(b)/7)C] for Metwork and Infrastructure Services for MIT exiting them to further pinpoint the location of the computer downloading the journals. At 0000 [Di(6),(b)/7)C] for Metwork and Infrastructure Services for MIT exiting them to further pinpoint the location of the computer is also commetted to an external hand drive. [Di(6),(b)/7)C] establish a packet capture of the same switch the computer is found attented to. On 01/04/11, Detective [Di(6),(b)/7)C] of the Cambridge Police Department and a member of the Rew Registed Electronic Crimes Task Force received a call from [Di(6),(b)/7)C] [DIT TEOT) of the Messachusetts Institute of Technology Police Department that an unauthorized computer had been found in a wire closet on MIT grounds and Network Traffic sugasted that the computer was being used to download expansive technical jour	On 10/12/10, the MIT Network and Information Security Team received an enall from
On 10/13/10, \(\(\) \(
downloading to a computer registered on the network as "Grace Rost" with an email of ghost-28mailinator com, a NAC address of 0017f22cb074 and computer name of "ghost-laptop". [0](0](0) disabled the host registrations identified as bogus. [0](0](0)(7)(C) had 0(0)(C) [the 0(7)(C)] hir contified[0](0](0)(7)(C) had 0(0)(7)(C) hir contified[0](0](0)(7)(C) had 0(0)(7)(C) hir contified0(0)(7)(C) had 0(0)(7)(C) hir contified by the NIT notified0(0)(0)(0)(C) hir continue and information and information in building 16. On 11/29/10, the MIT Network and Information Security Team is notified by the NIT branch of the Institute of Electrical and Electronic Engineers that journal spidering is occurring on their site and it is tracked to the Student Information Processing Board XVM cluster, a group of computers that are shared and that anyons in the NIT community can host a Virtual Machine on. On 11/30/10, the Virtual Nachine downloading journals from JSTCR is taken offline. On 01/03/11 at approximately 1440, 0(0)(7)(C) received an email from 0(0)(0)(1)(1) informing him that that the excessive downloading of journals had begun again. (b)(6)(0)(7)(C) and 0(0)(7)(C) and 0(0)(7)(C) the NIT and 0(0)(0)(7)(C) and 0(0)(7)(C) the NIT asking them to further pinpoint the location of the computer downloading the journals. At 0808 [0](6)(0)(7)(C) the NIT and [0](6)(0)(7)(C) and [0](6)(0)(7)(C) are alloaded by a box connected to a switch in a wire closet in the basement of building 16. The computer downloading the journals. At 0808 [0](6)(6)(7)(C) are alloaded aspensive to the Cambridge Police Department and a member of the Naw Regland Bloctronic Crimes Task Force received a call from [0](6)(6)(6)(7)(C) hirt. EDD1 of the Massachusetts Institute of Tochnology Police Department that an unauthorized computer had been found in a wire closet on NIT grounds and Metwork Traffic suggested that the computer was being used to download expensive technical journals without authoriza	
downloading to a computer registered on the network as "Grace Rost" with an email of ghost-28mailinator com, a NAC address of 0017f22cb074 and computer name of "ghost-laptop". [0](0](0) disabled the host registrations identified as bogus. [0](0](0)(7)(C) had 0(0)(C) [the 0(7)(C)] hir contified[0](0](0)(7)(C) had 0(0)(7)(C) hir contified[0](0](0)(7)(C) had 0(0)(7)(C) hir contified0(0)(7)(C) had 0(0)(7)(C) hir contified by the NIT notified0(0)(0)(0)(C) hir continue and information and information in building 16. On 11/29/10, the MIT Network and Information Security Team is notified by the NIT branch of the Institute of Electrical and Electronic Engineers that journal spidering is occurring on their site and it is tracked to the Student Information Processing Board XVM cluster, a group of computers that are shared and that anyons in the NIT community can host a Virtual Machine on. On 11/30/10, the Virtual Nachine downloading journals from JSTCR is taken offline. On 01/03/11 at approximately 1440, 0(0)(7)(C) received an email from 0(0)(0)(1)(1) informing him that that the excessive downloading of journals had begun again. (b)(6)(0)(7)(C) and 0(0)(7)(C) and 0(0)(7)(C) the NIT and 0(0)(0)(7)(C) and 0(0)(7)(C) the NIT asking them to further pinpoint the location of the computer downloading the journals. At 0808 [0](6)(0)(7)(C) the NIT and [0](6)(0)(7)(C) and [0](6)(0)(7)(C) are alloaded by a box connected to a switch in a wire closet in the basement of building 16. The computer downloading the journals. At 0808 [0](6)(6)(7)(C) are alloaded aspensive to the Cambridge Police Department and a member of the Naw Regland Bloctronic Crimes Task Force received a call from [0](6)(6)(6)(7)(C) hirt. EDD1 of the Massachusetts Institute of Tochnology Police Department that an unauthorized computer had been found in a wire closet on NIT grounds and Metwork Traffic suggested that the computer was being used to download expensive technical journals without authoriza	On 10/13/10, (D)(0),(D) traced the second occurrence of excessive unauthorized
eghost-laptop. [0](0](0)(0) disabled the host registrations identified as hogus. [5](0](0](0)(1)(C) hemoger of [6](0](0](0)(1)(C) for notifies[0](0](0](0)(0)(1)(C) the [0](0](0)(0)(1)(C) MIT Operations and Infrastructure that information indicates that the same unknown person appears to be using MIT guest registration from a wired connection in building 16. On 11/29/10, the MIT Metwork and Information Security Team is notified by the MIT branch of the Institute of Electrical and Electronic Engineers that journal spidering is cocurring on their site and it is tracked to the Student Information Processing Board XVM cluster, a group of computers that are shared and that anyons in the MIT community can host a Virtual Machine on. On 11/30/10, the Virtual Machine downloading journals from JSTCR is taken offline. On 01/03/11 at approximately 1440, 0(0)(0)(0)(0) received an email from JSTCR is taken offline. On 01/04/11 at approximately 0249, 0(0)(0)(0) received an email from JSTCR is taken journals had begun again. (D)(0)(0)(7)(C)	downloading to a computer registered on the network as "Grage Host" with an email
bogus. (b)(0)(b)(7)(C) Ind (b)(0)(b)(7)(C) Interesting (b)(0)(b)(7)(C) MIT Operations and Infrastructura that information indicates that the same unknown person appears to be using MIT guest registration from a wired connection in building 16. On 11/29/10, the MIT Metwork and Information Security Team is notified by the MIT branch of the Institute of Electrical and Electronic Engineers that journal spidering is occurring on their site and it is tracked to the Student Information Processing Board XVM cluster, a group of computers that are shared and that anyone in the MIT community can host a Virtual Machine on. On 11/30/10, the Virtual Machine downloading journals from JSTOR is taken offline. On 01/03/11 at approximately 1440, (ONE)(DNIC) received an email from forwarded from (D(O)(D)(D) informing him that that the excessive downloading of journals had begun again. On 01/04/11 at approximately 0249, (D(O)(D)(T) mails (D(O)(D)(T)(C) and (D(O)(D)(T)(C) and (D(O)(D)(T)(C) the MIT setting them to further pinpoint the location of the computer downloading the journals. At 0808 (D(O)(D)(T)(C) the location of the computer downloading the journals. At 0808 (D(O)(D)(T)(C) or building 16. The computer is also connected to an external hard drive. (D(O)(D)(T)(C) stablish a packet capture of the same switch the computer is found attended to. On 01/04/11, Detective (D(O)(D)(T)(C) for the Massachusetts Institute of Technology Police Department that an unauthorised computer had been found in a wire closet on MIT grounds and Network Traffic suggested that the computer was being used to download expensive technical journals without authorization. The	of ghost42@mailinator.com, a MAC address of 0017f22cb074 and computer name of
Infrastructure that information indicates that the same unknown person appears to be using NIT guest registration from a wired commection in building 16. On 11/29/10, the MIT Metwork and Information Security Team is notified by the MIT branch of the Institute of Electrical and Electronic Engineers that journal spidering is occurring on their site and it is tracked to the Student Information Processing Board XVM cluster, a group of computers that are shared and that anyone in the MIT community can host a Virtual Machine on. On 11/30/10, the Virtual Machine downloading journals from JETOR is taken offline. On 01/03/11 at approximately 1440, [000,007/00] received an email from JETOR is taken offline. On 01/03/11 at approximately 1440, [000,007/00] received an email from JETOR is taken of forwarded from [000,00] informing him that that the excessive downloading or journals had begun again. (b)(0)(0)(0)(7)(0)	"ghost-lapton", (NORO)AD) disabled the nost registrations localitated as
Infrastructure that information indicates that the same unknown person appears to be using MIT guest registration from a wired connection in building 16. On 11/29/10, the MIT Metwork and Information Security Team is notified by the MIT branch of the Institute of Electrical and Electronic Engineers that journal spidering is cocurring on their site and it is tracked to the Student Information Processing Scard XVM cluster, a group of computers that are shared and that anyone in the MIT community can host a Virtual Machine on. On 11/30/10, the Virtual Machine downloading journals from JSTOR is taken offline. On 01/03/11 at approximately 1440, [0](0](0)(0)(0) received an email from forwarded from 0(0)(0)(1) informing him that that the excessive downloading GY journals had begun again. (b)(0)(0)(0)(7)(C)	notificative (507/2) and (b)(8)(b)(7)(C) the (b)(8)(b)(7)(C) MIT Operations and
On 11/29/10, the MIT Network and Information Security Team is notified by the MIT branch of the Institute of Electrical and Electronic Engineers that journal spidering is occurring on their site and it is tracked to the Student Information Processing Board XVM cluster, a group of computers that are shared and that anyons in the MIT community can host a Virtual Machine on. On 11/30/10, the Virtual Machine downloading journals from JSTOR is taken offline. On 01/03/11 at approximately 1440, [00/01/01/07] received an email from [60/01/06] informing him that that the excessive downloading or journals had begun again. On 01/04/11 at approximately 0249, [60/01/05/07] [60/01/07/07] the MIT [50/01/06/07/07] and [60/01/06/07/07] init.edu) a [60/01/07/07] the MIT [50/01/06/07/07] and [60/01/06/07/07] init.edu) a [60/01/07/07] the MIT [50/01/06/07/07] and [60/01/07/07] init.edu) a [60/01/07/07] [60/01/07/07] for Metwork and Infrastructure Services for MIT sating them to further pinpoint the location of the computer downloading the journals. At 0000 [60/01/07/07] [60/01/07/07] for Metwork and Infrastructure Services for MIT sating them to further pinpoint the location of the computer downloading the journals. At 0000 [60/01/07/07] [60/01/07/07] for Metwork and Infrastructure Services for MIT sating them to further pinpoint the location of the computer is also commetted to an external hard drive. [60/01/07/07] [60/01/07/07/07/07] On 01/04/11, Detective [60/01/07/07/07/07] of the Cambridge Police Department and a member of the New England Electronic Crimes Teak Force received a call from [60/01/07/07/07/07/07/07/07/07/07/07/07/07/07/	Infrastructure that information indicates that the same unknown person appears to
branch of the Institute of Electrical and Electronic Engineers that journal spidering is occurring on their site and it is tracked to the Student Information Processing Board XVM cluster, a group of computers that are shared and that anyone in the MIT community can host a Virtual Machine on. On 11/30/10, the Virtual Machine downloading journals from JSTCR is taken offline. On 01/03/11 at approximately 1440,	be using MIT guest registration from a wired connection in building 16.
offline. On 01/03/11 at approximately 1440, 0(0)(7)(C) received an email from forwarded from 0(0)(0)(1) informing him that that the excessive downloading or journals had begun again. (b)(0)(0)(0)(7)(C) (b)(7)(C) (c) (b)(6)(b)(7)(C) (c) (d)(6)(b)(7)(C) (d)(6)(6)(6)(7)(C) (d)(6)(6)(6)(7)(C) (d)(6)(6)(6)(6)(6)(6)(6)(6)(6)(6)(6)(6)(6)	branch of the Institute of Electrical and Electronic Engineers that journal spidering is occurring on their site and it is tracked to the Student Information Processing Board XVM cluster, a group of computers that are shared and that
on 01/03/11 at approximately 1440, (0)(0)(0)(0)(1)(1) received an email from forwarded from (0)(0)(0)(0)(1) informing him that that the excessive downloading or journals had begun again. (b)(6)(6)(0)(7)(C) On 01/04/11 at approximately 0249 (b)(6)(b)(7)(c) (b)(6)(b)(7)(C) and(b)(6)(b)(7)(C) and(b)(6)(b)(7)(C) for Network and Infrastructure Services for NIT asking them to further pinpoint the location of the computer downloading the journals. At 0808 (b)(6)(b)(7)(C) (b)(6)(d)(d)(d)(d)(d)(d)(d)(d)(d)(d)(d)(d)(d)	offline.
forwarded from (D)(6),(b)(informing him that that the excessive downloading of journals had begun again. (b)(6),(b)(7)(C) Cn 01/04/11 at approximately 0249, (D)(6),(D)(7) emails (b)(6),(D)(7)(C) the MIT (b)(6),(D)(7)(C) and (D)(6),(D)(7)(C) for Network and Infrastructure Services for MIT asking them to further pinpoint the location of the computer downloading the journals. At 0808 (D)(6),(D)(7)(C) for Network and Infrastructure Services for MIT asking them to further pinpoint the location of the computer downloading the journals. At 0808 (D)(6),(D)(7)(C) locates a computer hidden by a box connected to a switch in a wire closet in the basement of building 16. The computer is also connected to an external hard drive. (D)(6),(D)(7)(C) establish a packet capture of the same switch the computer is found attached to. On 01/04/11, Detective (D)(6),(D)(7)(C) of the Cambridge Police Department and a member of the New England Electronic Crimes Task Force received a call from (D)(6),(D)(7)(C) MIT.EDU) of the Massachusetts Institute of Technology Police Department that an unauthorized computer had been found in a wire closet on MIT grounds and Network Traffic suggested that the computer was being used to download expensive technical journals without authorization. The	(b)(6),(b)(7)(C)
con 01/04/11 at approximately 0249. (b)(6).(b)(7)(c) the MIT (b)(6).(b)(7)(c) and (b)(6).(b)(7)(c) mit.edu) a (b)(6).(b)(7)(c) for Network and Infrastructure Services for MIT asking them to further pinpoint the location of the computer downloading the journals. At 0808 (b)(6).(b)(7)(c) locates a computer hidden by a box connected to a switch in a wire closet in the basement of building 16. The computer is also connected to an external hard drive. (b)(6).(b)(7)(c) establish a packet capture of the same switch the computer is found attached to. On 01/04/11, Detective (b)(6).(b)(7)(c) of the Cambridge Police Department and a member of the New Regland Electronic Crimes Tank Force received a call from (b)(6).(b)(7)(c) will EDU) of the Massachusetts Institute of Technology Police Department that an unauthorized computer had been found in a wire closet on MIT grounds and Network Traffic suggested that the computer was being used to download expensive technical journals without authorization. The	forwarded from (b)(6),(b)(informing him that that the excessive down (c)(1)(1)(1)
Cn 01/04/11 at approximately 0249. (b)(6).(b)(7)(C) mit.edu) a (b)(6).(b)(7)(C) mit.ed	journals had begun again.
for Network and Infrastructure Services for NIT asking them to further pinpoint the location of the computer downloading the journals. At 0808 (D)(5),(b)(1) locates a computer hidden by a box connected to a switch in a wire closet in the basement of building 16. The computer is also commetted to an external hard drive. (b)(8),(b)(1) establish a packet capture of the same switch the computer is found attached to. On 01/04/11, Detective (D)(6),(b)(7)(C) of the Cambridge Police Department and a member of the New England Electronic Crimes Task Force received a call from (D)(6),(b)(7)(C) NIT.EDU) of the Nessachusetts Institute of Technology Police Department that an unauthorized computer had been found in a wire closet on NIT grounds and Network Traffic suggested that the computer was being used to download expensive technical journals without authorization. The	
for Network and Infrastructure Services for MIT asking them to further pinpoint the location of the computer downloading the journals. At 0808 (b)(6),(b)(locates a computer hidden by a box connected to a switch in a wire closet in the basement of building 16. The computer is also commerced to an external hard drive. (b)(8),(b)(establish a packet capture of the same switch the computer is found attached to. On 01/04/11, Detective (b)(6),(b)(7)(C) of the Cambridge Police Department and a member of the New England Electronic Crimes Task Force received a call from (b)(6),(b)(7)(C) MIT.EDU) of the Massachusetts Institute of Technology Police Department that an unauthorized computer had been found in a wire closet on MIT grounds and Metwork Traffic suggested that the computer was being used to download expensive technical journals without authorization. The	
the location of the computer downloading the journals. At 0608 (b)(6),(b)(locates a computer hidden by a box connected to a switch in a wire closet in the basement of building 16. The computer is also commected to an external hard drive. (b)(6),(b)() establish a packet capture of the same switch the computer is found attached to. On 01/04/11, Detective (b)(6),(b)(7)(C) of the Cambridge Police Department and a member of the New England Electronic Crimes Task Force received a call from (b)(6),(b)(7)(C) MIT.EDU) of the Massachusetts Institute of Technology Police Department that an unauthorized computer had been found in a wire closet on MIT grounds and Network Traffic suggested that the computer was being used to download expensive technical journals without authorization. The	
of building 16. The computer is also commented to an external hard drive. (b)(6),(b)() establish a packet capture of the same switch the computer is found attacked to. On 01/04/11, Detective (b)(6),(b)(7)(C) of the Cambridge Police Department and a member of the New England Electronic Crimes Tank Force received a call from (b)(6),(b)(7)(C) MIT.EDU) of the Massachusetts Institute of Technology Police Department that an unauthorized computer had been found in a wire closet on MIT grounds and Network Traffic suggested that the computer was being used to download expensive technical journals without authorization. The	
drive. (b)(6),(b)() establish a packet capture of the same switch the computer is found attached to. On 01/04/11, Detective (b)(6),(b)(7)(C) of the Cambridge Police Department and a member of the New England Electronic Crimes Tank Force received a call from (b)(6),(b)(7)(C) MIT.EDU) of the Massachusetts Institute of Technology Police Department that an unauthorized computer had been found in a wire closet on MIT grounds and Network Traffic suggested that the computer was being used to download expensive technical journals without authorization. The	
found attached to. On 01/04/11, Detective (b)(6),(b)(7)(C) of the Cambridge Police Department and a member of the New England Electronic Crimes Tank Force received a call from (b)(6),(b)(7)(C) MIT.EDU) of the Massachusetts Institute of Technology Police Department that an unauthorized computer had been found in a wire closet on MIT grounds and Network Traffic suggested that the computer was being used to download expensive technical journals without authorization. The	
(b)(0),(b)(7)(C) MIT.EDU) of the Massachusetts Institute of Technology Police Department that an unauthorized computer had been found in a wire closet on MIT grounds and Network Traffic suggested that the computer was being used to download expensive technical journals without authorization. The	found attached to.
(b)(0),(b)(7)(C) MIT.EDU) of the Massachusetts Institute of Technology Police Department that an unauthorized computer had been found in a wire closet on MIT grounds and Hetwork Traffic suggested that the computer was being used to download expensive technical journals without authorization. The	On 01/04/11. Detective (b)(6),(b)(7)(C) of the Cambridge Police Department and a
(b)(6)(0)(7)(C) MIT.EDU) of the Massachusetts Institute of Technology Police Department that an unauthorised computer had been found in a wire closet on MIT grounds and Hetwork Traffic suggested that the computer was being used to download expensive technical journals without authorisation. The	member of the New England Electronic Crimes Tank Force received a call from
wire closet on MIT grounds and Hetwork Traffic suggested that the computer was being used to download expensive technical journals without authorisation. The	(b)(6),(b)(7)(C) MIT.EDU) of the Massachusetts Institute of
being used to download expensive technical journals without authorisation. The	
	computer was found in a wire closet of in the basement of Building 16, the

Dorrance Building (77 Massachusetts Avenue, Cambridge, MA) which houses MIT Biological Engineering Department. (b)(8),(b)(7)(C) Detective (7)(C) and Detective (b)(a),(b)(7) Also on 01/04/11, SA (b)(6),(b)(7)(of the Boston Police traveled to MIT and met with (b)(0),(b)(7)(C) (b)(6)(b)(7)(C) wit.edu) of the MIT Police, (b)(5)(b)(7) and (b)(6)(b)(1) in the basement of building 16. Cambridge Police processed the scene for prints. The netbook found connected to the switch in the wire closet in the basement of building 16 was an Acer Aspire One with a serial number LUSAKOD001001100E1601. The natbook matches the description of an Ager netbook (0)(8),(0)(7)(C) reported as stolen to MIT Police on 12/31/10. Network traffic indicated that the netbook was using two IP address (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) which are both IP addresses belonging to MIT. Use of NNap showed that the netbook had port 22 and 8092 open. Port 22 is the default port for SSH (Secure Shell network protocol) and port 8092 that is often associated with TCP (Transmission Control Protocol) traffic. A surveillance camera was placed in the wire closet to record anyone returning for the netbook. Also on 01/04/11, at approximately 1526, the surveillance camera was able to record a white male later identified as Aaron Swartz (DOB 11/08/86) enter the wire closet. Based on the surveillance video Swartz appeared to replace the external hard drive with a new one and take the old hard drive with him. Also on 01/04/11, (7)(C) (b)(6),(b) also on 01/04/11, [7](C) provided SA [7](C) with a copy of historical network flow data concerning IP addresses [(b)(6),(b)(7)(C)] and [(b)(6),(b)(7)(C)] from 12/14/10 to 01/04/11 and DECP log information for computers registered as ghost-macbook and ghost-laptop. sa[b)(8),(b)(7] contacted sa(b)(8),(b)(7)(C) (CID) at the CERT Coordination Center at the Software Engineering Institute at Carnegie Mellon University, SA (b)(6),(b)(7) provided SA((b)(6),(b) with instructions to upload the data to the CERT drop On 01/06/11, at approximately 1232, video surveillance viewed the individual later identified as Swartz return to the wire closet and remove the netbook and external hard drive. At approximately 1411 (b)(8),(b)(7)(C)

of the MIT police Department called (b)(8),(b)(7)(C) of the MIT Folice and stated that he had located the suspect later identified as Swarts riding his bicycle on Massachusetts Avenue near the intersection with Lee Street in Cambridge Massachusetts. (6)(6),(6)(7)(C) and SA (6)(8),(6)(7) responded to Lee Street to assist (b)(d),(b)(7)(C) attempted to interview the Swartz however; Swartz jumped off of his bicycle and ran down Lee Street. (b)(6),(b)(7)(C) and SA (b)(6),(b)(7)(f) detained the suspect. An inventory of the backpack the suspect was wearing located a US passport in the name of Aaron Swarts. Swartz was transported by Cambridge Police to Cambridge Police headquarters to be booked for Breaking and Entering. Also on 01/06/11, (7)(C) checked the DECP logs for computer registrations with containing the word ghost. Ghost-laptop is seen to be still active on the MIT mit.edu) an MIT Network Engineer, traces ghost-laptop on the network to huilding W20 on the 5th floor. MIT Building W20 is the Stratton Student Center. (b)(8),(b)(7)(C) and (b)(8),(b)(1) network using the same MAC address as used on 01/04/11 to download journals. (b)(6),(b) Student Center and determined that the Network Drop Location ghost-laptop was connected to was in the Student Information Processing Board office, room 557. (b)(6).(b)(7)(contacted (b)(6),(b)(7)(C) to inform him that they believed they had traced the netbook to a room in the student center. SA (b)(6),(b)(7) met (b)(6),(b)(7) and (b)(6),(b)(7)(C) at the student center and found the Acer Aspire netbook and external hard

	(b) (b)(6),(b)(7)(C) (b)(6),(b)
Thu 9/30/10	pm emails end(7)(C) to provide the facts of the event
mentions th	
	(b)(6), and(b)(7) had spoken regarding possible solution utilizing authentication
that's	
	already available from the Libraries for JSTOR access; some logistics to work out
	(b)(6),
	11:15pm $(b)(7)$ emails (0) informing her MIT's JSTOR access has been cut off
again due to	
	downloading,
34 40014	(b) (b) (c)
Mon 10/11/	
raises issue	or 1910K
	sending in IP abuse information in timely manner vs. blocking all of MIT's access
anggests	t di. t
	additional measures of blocking due to lack of IP info as VPN-based abuses of
resources ju	
	exploited in the past.
5 40/46/4	(b)
Tue 10/12/1	0 6:36am Security team receives email from (6).(b regarding most recent JSTOR
abuse; no IP	
	information yet to act on.
-	(6)
Tue 10/12/10	0 4:02pm Security team receives email from (6).(b) with logs and IP address
information	provided by JSTOR.
•	151 Ok aboes resured. Abuse coming from address
	(b)(8), $(b)(b)(b)(6)$
Wed 10/13/1	(U) 6:34cm((D)(7)(sends email tol(8),(land(b)(7) regarding more info on further
pogns tegisti	ration information.
	Will press JSTOR to have brief technical conversation with JSTOR's
folks. Sugge	ess if our
	proxy solution already in place for other resources is utilized, it's possible that
ISTOR can	
1	automatically push people through it who attempt to access ISTOR directly so a
large behavio	27
	change doesn't inconvenience MIT community accessing ISTOR and there would
be authentica	tion
	to the resource.
	Host registration committing download now shows Grace Host
abost42@m	eilinetor.com).
	NA SAME STATEMENT OF SAME
	We saw Gary Host registered on 9/27 using MAC address 00235a735ffb (ghost-
nacbook).	
	We saw Grace Host registered on 10/9 using MAC address 0017f22cb074 (ghost-
aptop).	:
	We saw MAC addresses change, something that a person does typically to avoid
eing banned	or .
	tracked on network.
	We saw short-machook change to 00215471566 when hains beyond

IT	Security System	ems & Services, IS&	Γ		
	m				
(6),(b)(7)(C)				
	***************************************	(b)(6),(b)(7)			
P	3P public key	D(C) Interes	thom mit edu		
***	BEGIN POL	SIGNATURE-			
(6)(6	(D)(7)(C)				4670
- 1					
- 1					
- 1					
<u> </u>	TATO POP S	CNATURE-		 	

	(b)(3):Rule 8E	per EOUSA
From: (SOS) [mailto] Sept: Thursday, January 06, 2011 2:09 PM Tel(b)(6),(b)(7)(C)),(b)(7)(C) pess.dhs.gov]	
How could I get a copy of the network traffic? (b)(8),(b)(7)(C) Sent from Blackberry		
Proma (b)(6),(b)(7)(C)	mit.edu>),(b)(7)(C) pmit.edu>	
Thank you	(b)(3):Rule 6E	per EOUSA
(b)(6),(b)(7)(C) Network & Infrastructure Information Services and Technology (IS&T) Massachusetts Institute of Technology Room(b)(0),(b)(7)(C) Cambridge, MA 02139 (b)(6),(b)(7)(C)	Services	

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further discerninated without the permission of the Secret Service. If you have

	•
····	

All e-mail to/from this assount is subject to official review and is for official use only. Action may be taken in response to my inappropriate use of the Secret Service's e-mail system. This e-mail may contein information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the parallelos of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

		(b)(a),(b)(7)(c)	MET.EDU>		
Proms Sent:	ìđ	Friday, January 07, 20			
Tec	(b)(6),(b)(7)(C)			1049
Cc:	(b)(8),(b)(7)(C		<u>051</u>		12
Subject		1st hard drive from s	uspect		
BEGIN PGP S Hash: SHA1	GNED MESSAGI	[*	
swapped out by	the suspect on 1	g potentially recovering residency not property might be sittle	g the hard drive that was be most at this point if i is	s reported seen, on he's already been be	the video feed, being died out, but I'd think
I'm super impres time for you sil.	sed with all the	good work that went i	into this coming together	. Hopefully it work	ilike this most of the
Best , (b)(d).(b)(
(b)(8),(b)(7)(C)					
	s	ecurity Analyst IT Secu	rity Systems & Services A	AIT	
PGP Fingerprint:	(b)(8),(b)(7)(C)				
BEGIN PGP S	GRATURE				
(DYOYDK, YO)					

Prom:	(b)(d),(b)(7)(C)	ATT.EDU>
Sout	Thursday, January 05, 2011	
To:	(b)(8),(b)(7)(C) (C)	
Subject	Leptop Movement	
After returning	from Building 16, I checked radius logs and fou	und the
following entries	E	
perimeter:		
(b)(6),(b)(7) port	:08 2011 : Auth: Login OK: [004ce5e0c756] (fr 50023 cil 00-4C-E5-A0-C7-56)	ram client
tangent:	:52 2011 : Auth: Login OK: 00-4C-E5-A0-C7-56	A Constitution of the Cons
sector:		
Thu Jan 6 13:28	:53 2011 : Auth: Login OK: [00-46-25-A0-67-56	6] (from client((b)(6),(b)(7) port 7 di 00-4C-E5-A0-C7-56
We arrived at W	ed in Building 4, then W20. I checked the swit 20 and traced the jacks to a drop in W20-557. is being processed.	itch in W20 and found it still active. • MIT Police detectives arrived and found the leptop in
→		
(D)(8) (D)(7)(G)	Network Admin	
	estitute of Technology	
(b)(6),(b) mit.e		
		•
	(b)(6),(b)(7)(C)	
(6)(6),(5)(7)(C)	Network Admin	
	stitute of Technology	
mite	M I	

(b)(6),(b)(7)(C)

> All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, disclose, or copy it; notify the sender immediately and delete it. <12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-40.jpg><12-32-

BEGIN PGP SIGNATURE	
(D)(D),(D)(C)(C)	
31	
THE OCE CIGUATI IS	

(b)(6),(b)(7)(C)		
Prem:	NIT.EDU>	and the second second
Te (b)(8),(b)(7)(C)	BOS)(b)(8),(b)(7)(C)	bmit.edu>
Ca(b)(6),(b)(7)(C)	mlt.edu>{(b)(6),(b)(7)(C) httedu>
Sent: Wed Jan 05 17:		
Subject: Packet Capt		

Hi there.

I have collected about 70G of network treffic so fer with about 99% of which is the JSTOR journal downloads. I've done some initial checking of the capture and I don't see anything that identifies a command and control channel. I was just wondering what the next step is.

	nk you ,(b)(7)(C)
	Network & Infrastructure Services
Info	rmation Services and Technology (IS&T)
	sachusatts institute of Technology
	m (D)(e),(D)(7)(C)
Cam	bridge, MA 02139
	(b)(7)(C)
(b)(8), (b)(7) (C)	nit.edu

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, discloss, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

Sent: Thursday, January 06, 2011 3:22 PM Tes [(b)(6),(b)(7)(C) Subject: RE: Packet Capture Hi there, I've setup a web server on the machine containing the files so you can download them. They are in a standard topdum format. The LIRL is [(b)(3):Rule 8E We've got plenty of bandwidth over here, knowner, if downloading this much data is a problem for you i could put the on a SATA drive and bring them down to your office. Let me know.	Proste:		(b)(6),(b)(7)(C)	MIT.EDU>	
Tee: (D(B)(b)(F)(C) (RE PRESET Capture If there, I've setup a web server on the machine containing the files so you can download them. They are in a standard topdure formet. The Lift is (D(B)(Rule BE) We've got planty of bandwidth over there, however, if downloading this much data is a problem for you i could put the on a SATA drive and bring them down to your office. Let me know. Thanks: (D(B)(B)(D(T)(C)) (D(B)(B)(B)(B)(B)(B)(B)(B)(B)(B)(B)(B)(B)(Sent:		Thursday, January		
Hi there, I've setup a web server on the machine containing the files so you can download them. They are in a standard topdure format. The URL is (DIGISRUIS DE We've got planty of handwidth over here, however, if downloading this much data is a problem for you i could put the on a SATA drive and bring them down to your office. Let me know. Thanks (b(6),(b)(7)(C) (b(6),(b)(7)(C) (b(6),(b)(7)(C) (b(6),(b)(7)(C) (b(6),(b)(7)(C) (b(6),(b)(7)(C) (c)(b),(b)(7)(C) (c)(b),(b)(7)(C) (c)(b),(b)(7)(C) (c)(b),(b)(7)(C) (c)(b),(b)(7)(C) (c)(b),(b)(7)(C) (c)(b),(b)(7)(C) (c)(b),(b)(7)(C) (c)(b),(b)(7)(C) (c)(c)(c)(c)(c)(c)(c)(c)(c)(c)(c)(c)(c)(Tes	(EV6) (_	
I've setup a web server on the machine containing the files so you can download them. They are in a standard topdum format. The URL is (5(3):Rule BE) We've got plently of handwidth over here, however, if downloading this much data is a problem for you i could put the on a SATA drive and bring them down to your office. Let me know. Thanks (b)(6)(b)(7)(C) Present (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) Present (b)(6)(b)(7)(C) (c)(c)(c)(c)(c)(c)(c)(c)(c)(c)(c)(c)(c)(Subject:	(10)(10)(1	RE: Packet Capture	(20)	
I've setup a web server on the machine containing the files so you can download them. They are in a standard topdum format. The URL is (5(3):Rule BE) We've got plently of handwidth over here, however, if downloading this much data is a problem for you i could put the on a SATA drive and bring them down to your office. Let me know. Thanks (b)(6)(b)(7)(C) Present (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) Present (b)(6)(b)(7)(C) (c)(c)(c)(c)(c)(c)(c)(c)(c)(c)(c)(c)(c)(•				
I've setup a web server on the machine containing the files so you can download them. They are in a standard topdum format. The URL is (5(3):Rule BE) We've got plently of handwidth over here, however, if downloading this much data is a problem for you i could put the on a SATA drive and bring them down to your office. Let me know. Thanks (b)(6)(b)(7)(C) Present (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) Present (b)(6)(b)(7)(C) (c)(c)(c)(c)(c)(c)(c)(c)(c)(c)(c)(c)(c)(Hi there.				*
Format. The Lift is [D(0);Ruis BE We've got planty of bandwidth over here, however, if downloading this much data is a problem for you i could put the on a SATA drive and bring them down to your office. Let me know. Thanks (b)(6),(b)(7)(C) [B(5)] [meltio [b server on the	machina containine ti	se files so you can download ti	nom. They are in a standard tendum
We've got planty of bandwidth over here, however, if downloading this much data is a problem for you i could put the on a SATA drive and bring them down to your office. Let me know. Thanks (b)(8),(b)(7)(C) (BOS) [molito Presse (b)(8),(b)(7)(C) (BOS) [molito (b)(8),(b)(7)(C) (BOS) [molito (b)(8),(b)(7)(C) (BOS) [molito (b)(8),(b)(7)(C) (BOS) [molito (b)(8),(b)(7)(C) (b)(8),(b)(7)(C) (b)(8),(b)(7)(C) (BOS) (b)(8),(b)(7)(C) (b)(8),(b)(8),(b)(8)	format. The UR	il is		or many and long arms and stress of	inemia ine al a etalicale celarii
Thanks (b)(8),(b)(7)(C) Preme (b)(8),(b)(7)(C) Prem	(b)(3):Rule 8E			*	
Thanks (b)(8),(b)(7)(C) Preme (b)(8),(b)(7)(C) Prem					
Thanks (b)(8),(b)(7)(C) Preme (b)(8),(b)(7)(C) Prem	Walus ant ninn	w all handwide	have been become	W daniel and an this words date	Jan - and law flammed and discussed
Thanks (b)(6),(b)(7)(C) (BOS) [metto] (b)(6),(b)(7)(C) (BOS) [metto] (c)(6),(b)(7)(C) (BOS) [metto] (c)(6),(b)(7)(C) (c)(6),(b)(7)(C) (c)(6),(b)(7)(C) (c)(6),(b)(7)(C) (c)(6),(b)(7)(C) (c)(6),(b)(7)(C) (c)(6),(b)(7)(C) (c)(6),(b)(7)(C) (c)(6)(6),(b)(7)(C) (c)(6)(6)(6)(6)(6)(6)(6)(6)(6)(on a SATA drive	and bring the	m down to your office	i gowingsping this mych gag tat ma know	is a problem for you I could put the
(b)(0),(b)(7)(C) Preset (b)(0),(b)(7)(C) (b)(0),(b)(7)(C) (b)(0),(b)(7)(C) (b)(0),(b)(7)(C) (b)(0),(b)(7)(C) (b)(0),(b)(7)(C) (c)(d)(d)(d)(d)(d)(d)(d)(d)(d)(d)(d)(d)(d)			water, on lane avelant,	DOLLING MINAE.	
Prene (b)(6),(b)(7)(C) (BOS) [mailto] (b)(6),(b)(7)(C) (b)(d)(d)(d)(d)(d)(d)(d)(d)(d)(d)(d)(d)(d)	Thanks		•	•	
Personal		(b)(8),(b)(7)	(C)		
Personal					
Register Net Petrez Capture How could I get a copy of the network traffic? b)(8),(b)(7)(C) Sent from Blackberry Frequent (b)(8),(b)(7)(C) Frequent (c)(8),(b)(7)(C) Frequent (c)((b)(d),(b)	, ,, ,		C)	
(b)(6),(b)(7)(C) Sent from Blackberry How could I get a copy of the network traffic? (b)(6),(b)(7)(C) Sent from Blackberry How (b)(6),(b)(7)(C) MIT ED1> How (c)(6),(b)(7)(C) MIT ED1> How (c)(6),(c)(6),(c)(7)(C) MIT ED1> How (c)(6),(c)(7)(C) M	Frent	(80	S) [mailto	vusss.dhs.gov]	
How could I get a copy of the network traffic? (b)(6),(b)(7)(C) Sent from Blackberry (b)(6),(b)(7)(C) (BDCS),(b)(6),(b)(7)(C) (BDCS),(b)(7)(C) (BDCS),(b)(6),(b)(7)(C) (BDCS),(b)(6),(b)(7)(C					
How could get a copy of the network traffic? Sent from Blackberry Press (b)(8),(b)(7)(C) Press (c)(8),(b)(7)(C) P			DK! NO!		
Sent from Blackberry (b)(6),(b)(7)(C)					
Sent from Blackberry Prem (b)(8),(b)(7)(C) (BOS).(b)(6),(b)(7)(C) (BOS).(b)(6),(b)(7)(C) (BOS).(b)(6),(b)(7)(C) (BOS).(b)(6),(b)(7)(C) (BOS).(b)(6),(b)(7)(C) (BOS).(b)(6),(b)(7)(C) (BOS).(b)(6),(b)(7)(C) (BOS).(b)(6),(b)(7)(C) (BOS).(b)(7)(C) (BOS).(b)(7)(C	How could I get	a copy of the r	etwork traffic?		
Sent from Blackberry Prem (b)(8),(b)(7)(C) (BOS).(b)(6),(b)(7)(C) (BOS).(b)(6),(b)(7)(C) (BOS).(b)(6),(b)(7)(C) (BOS).(b)(6),(b)(7)(C) (BOS).(b)(6),(b)(7)(C) (BOS).(b)(6),(b)(7)(C) (BOS).(b)(6),(b)(7)(C) (BOS).(b)(6),(b)(7)(C) (BOS).(b)(7)(C) (BOS).(b)(7)(C	5V8) (5V7)(C)	1			
(b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) mit.edu> (b)(8),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) mit.edu> (b)(8),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) mit.edu> (b)(8),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) mit.edu> (b)(8),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C) mit.edu> (c)(6),(b)(7)(C) mit.edu> (c)(6),(b)(7)(C		Ì			¥
Promotion Services and Technology (IS&T) Interest	Donald days and the	•			•
her (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) miledu> c(b)(6),(b)(7)(C) [6miledu>(b)(6),(b)(7)(C) miledu> c(b)(6),(b)(7)(C) [6miledu>(b)(6),(b)(7)(C) miledu> continued Jan 05 17:01:53 2011	SHIRE HOLD ESTROIG	beny			
her (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) miledu> c(b)(6),(b)(7)(C) [6miledu>(b)(6),(b)(7)(C) miledu> c(b)(6),(b)(7)(C) [6miledu>(b)(6),(b)(7)(C) miledu> continued Jan 05 17:01:53 2011	DEVICE V	31/21			
ins((b)(6),(b)(7)(C)	**************************************	/ <u>/</u> (C)	MITEMA		
if there, have collected about 70G of network traffic so far with about 98% of which is the ISTOR journal downloads. I've done ome initial checking of the capture and I don't see anything that identifies a command and control channel. I was just condering what the next step is. hank you Network & Infrastructure Services Network institute of Technology (IS&T) Inspection (IS&T)	(b)(6),(b)(7)(0	(BOS):	b)(6),(b)(7)(C)	mit.edu>	200
Pathylact: Packet Capture If there, have collected about 70G of network traffic so far with about 98% of which is the ISTOR journal downloads. I've done ome initial checking of the capture and I don't see anything that identifies a command and control channel. I was just wondering what the next step is. Thank you Bletwork & Infrastructure Services Information Services and Technology (IS&T) Insesschumetts institute of Technology Config. (IS&T)		}	(D)(T)(O),(D)(T)(C	mkedu>	
fithere, have collected about 70G of network traffic so far with about 98% of which is the ISTOR journal downloads. I've done ome initial checking of the capture and I don't see anything that identifies a command and control channel. I was just wondering what the next step is. Thank you (b)(7)(C) Network & Infrastructure Services Iformation Services and Technology (IS&T) Isssechments institute of Technology COM (IS&T)		<i>15</i> 17:01:53 20	11		
have collected about 70G of network traffic so far with about 98% of which is the ISTOR journal downloads. I've done ome initial checking of the capture and I don't see anything that identifies a command and control channel. I was just condering what the next step is. thank you Network & Infrastructure Services Network & Infrastructure Services	resignate Packet	Capture			
have collected about 70G of network traffic so far with about 98% of which is the ISTOR journal downloads. I've done ome initial checking of the capture and I don't see anything that identifies a command and control channel. I was just condering what the next step is. thank you Network & Infrastructure Services Network & Infrastructure Services	li there.				
tione initial checking of the capture and I don't see anything that identifies a command and centrol channel. I was just wondering what the next step is. Thank you 6),(b)(7)(C) Network & infrastructure Services Iformation Services and Technology (IS&T) Isssechments institute of Technology com (IS&I)(IS)(IS)(IS)(IS)		about 70G of n	ebwork traffic so for wi	th shout GRK of which is the I	CTAB laurent deumlande. Von dage
hank you 6),(b)(7)(C) Network & Infrastructure Services iformation Services and Technology (IS&T) fassachmotts institute of Technology com (ESO)(D)(7)	cuse midel cust	said of the col	iture and i don't see an	withing that identifies a comm	and and control channel. I was but
Network & Infrastructure Services Iformation Services and Technology (IS&T) Isssechmotts institute of Technology com (IS&I)(IS&I)	vondering what	the next step	is.		- The second of
Network & Infrastructure Services Iformation Services and Technology (IS&T) Isssechmotts institute of Technology com (IS&I)(IS&I)	hank was				8
Network & Infrastructure Services iformation Services and Technology (IS&T) flassechusetts institute of Technology com (IS&I)(IS)(I)	<u> </u>				
iformation Services and Technology (IS&T) lassechments institute of Technology com (ISB)(I)(I)	5),(b)(7)(C)				
iformation Services and Technology (IS&T) isssechungtts institute of Technology com (5(8),(5)(7)		Network &	Infrastructure Services		
com (D)(U)(D)(Y)		ices and Techn	alogy (IS&T)		9
COMPANIES.	lossechusotts in	guitute of Tech	nology		
	COMPONDIANT)]			

(b)(8),(b)(7)(U.S. Secret B Boston Field Francis (C) Scart: Thurs Tep((b)(6),(b) C	خ)			
U.S. Secret S Boston Pield				
	(DIOXDXVIC)			
(b)(6)	(b)(7) (b)(6),(b) (malke)(7)(C)	WIT.EDU)	W 1-4-4 1 M M M M M M M M M M M M M M M M M M	W
Sent: Thurs To:(b)(6),(b	lay. January 06, 2011 9:37	ZAM (6)(8),(6		
C C	(<i>1)</i> (C)	(BOS): External (7)(C)		
Stage of M	T - BM 16			
All,				
I am going to	suggest that we take the	leptop and hard drive offic	na today. I think the amount of network t	
 captured is s 	ufficient and would like to	remove the lastos to see i	If he comes back to retrieve it. I will be at	ranno Na to put
some people	there for a short time in a	in attempt to ID.		
I am followir	g up a couple of possible !	D's this morning and will go	et back to you on my success (or not).	
The open qu	estions will be if we decide	to take it offline, is this so	mathing i can do with instruction or will i	need help?
Also, do we	vant to have the new drive	printed?		
(b)(ð), (b)(7)(Â.		
	(b)(7)(C)	- ANN AMALE	***************************************	
Promis Santa Wedn	sday, January 05, 2011 5:	02 PM		
Te*(b)(6),(b)(7	$7)(C)$ uses the $aowl(b)(\theta)$),(b)(7)(C)		
Subjects Pa				
Hi there.				
I have collect	ed about 709 of network t	raffic so far with about 989	K of which is the JSTOR journal download	s. I've done
अवसम्बद्धाः व्यवस्थाः	hecking of the capture and hat the next step is.	I don't see anything that i	dentifies a command and control channe	i. I was just
20 20000000 30 0	was train outplus			
Thank you				
(b)(6),(b)(7)(C)				
	Network & Infrastru			
	ervices and Technology (IS a institute of Technology	at)		
Room (D)(8),(b)	7)			
(b)(6),(b)(7)(C)	A 02139			
)(6),(b)(7) mit.edu	Į.			
2				

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is lossed to you and should not be further discensisted without the permission of the Secret Service. If you have

From:	(b)(6),(b)(7)(C)
Sent	Thursday, January 06, 2011 2:11 PM
To:	(b)(6),(b)(7)(C) BOS(b)(6),(b)(7)(C) External-
,	(b)(8),(b)(7)(C) cambridgepolice.org
Ce	(b)(8),(b)(7)(C)
Subject:	RE: When to pull laptop
(b)(6),(b)(7)(C) the video archi	(b) called me. He left a message with (6) . We saw the port go down at 12:32pm today. I'm going to look at ive. Did someone take this down intentionally?
(b)(6), (b)(7)(C)	· ·
/5\/A\/5\/5\/ M	
	etwork Operations ts Institute of Technology
	setts Ave, Room (DK6XDK7KC)
Cambridge. I	
Phone:	(b)(6),(b)(7)(C)
Email (b)(6),(1+ Adu
Victoria Commission (Commission Commission C	
———(b)(8),(b	(BOS) [melito vess.chs.gov]
Promi	(BOS) [melitousos.dhs.gov]
Ted(b)(6),(b)(7	(C) scambridgengics.org
Cd	(b)(8),(b)(7)(C)
	in to pull liptop
essilent anne	it on hom subsorb
What time wa	rks for you to pull the laptop and external? I am in my Boston office now. I could be there in 15. I would
like to keen the	ie surveillance camera running because I think he will come back when he notices the laptop is offline. Is
there are char	nce we could dust for prints again before we pull the laptop since we know he came back?
(b)(8),(b)(7)(C)	
U.S. Secret Serv	uriana
Boston Field Of	
),(b)(7)(C)	
(b)(6),(t	(b)(7), (b)(8), (mailto(b)(7)(C) (MIT.EDU)
	Pr. January Os. 2011 9:37 AM ((b)(8).(b))
Te (b)(6),(b)(7)	nr. January 06, 76(1 9:37 AM (C) (BOS); External (7)(C) cambridgepolics.org
Ce	(b)(8),(b)(7)(C)
Sublage Nut	
AM	

I am going to suggest that we take the laptop and hard drive offline today, I think the amount of network traffic captured is sufficient and would like to remove the laptop to see if he comes back to retrieve it. I will be able to put some people there for a short time in an attempt to ID.

i em following up a couple of possible ID's this morning and will get back to you on my success (or not).

The open questions will be if we decide to take it offline, is this something I can do with instruction or will I need help? Also, do we want to have the new drive printed?

(b)(7) (b)(6),(b)(7)(C) dneeday, January 05, 2011 5:02 PM (b)(6),(b)(7)(C) To((b)(6).(b)(7)(C))uses.dhs.gov (b)(8),(b)(7)(C) ok Packet Capture Hi there, I have collected about 70G of network traffic so far with about \$8% of which is the JSTOR journal downloads, i've done some initial checking of the capture and I don't see anything that identifies a command and control channel. I was lust wondering what the next step is. Thank you (b)(6),(b)(7)(C) **Network & Infrastructure Services** Information Services and Technology (IS&T) Massachusetts Institute of Technology Room (D)(0),(D)(7)(C) (b)(6),(b)(7)(C) (b)(8),(b) mit.edu

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

		6),(b)(7)(C)			
	(D)(t		cambridgepolice.org	1>	
From: Sent:	Thi	ursday, January 06, 2		2 4 4	
To:	(b)(6),(b)(7)(C	MIT.EDU			
Cc:		6),(b)(7) (b)(6),(b)(7)(C) BOS)		
Subject:	(C)	: MIT - Bid 16			
amject:	110	. IVILI - DIG AD			
(A)		(b)			
(b) (6),(that is certainly	vour cell and sour	inde good (6), will b	e responding either way.		
(O)// Indic to condensi	· John Odn Gira Boar	MON HOUSE			
(b)(6),(b)(7)(C)				
From		EDU>			
Ta (b)(6),(b)(7)(C)					
Cc: (b)(6),(b)(7)	100				
Sent: Thu Jan 06	11:17:02 2011				
Subject: RE: MIT	- Bld 16				
(b)(6)					
/h\/7\/h\We can had	tag and deliver if t	that works. I am thin	ring that if we are leaving	g the camera up, we should be	in an
out rather quickly	incase the suspect	t ventures by. I would	imagine (b)(6), could p	rocess it in her lab.	
, ,					
(b)(6).					,
	/EV/AV	/b\	N PERSON BOX - I NO SERVICIAL CO		
(b)(6),(b)(7)	(C) (b)(6), mailto(7)(C)		omi	=11000000000000000000000000000000000000	
	anuary 06, 2011 1:				
(b)(6),(b)(7)(C)	andary ovy money a.		o)(7)(C)		
Cci(b)(6),(b)(7)(C)		usss.dhs.gov';		acomcast.net';	
)(6),(b)(7)(C) JISSS	.dhs.gov'	•	•		- 1
V(0)(0)(1)(0) hpgs	10110100				
Subject: Fw: MIT					
Subject: Fw: MIT					
Subject: Fw: MIT (b)(6),(b)(7)(C)	- Bkd 16	na incantination to da			
Subject: Fw: MIT (b)(6),(b)(7)(C)	- Bkd 16	ne investigation to da	æ.	(b)(6),(b)(7)	
Subject: Fw: MIT (b)(6),(b)(7)(C) The thread below	- Bld 16 has the status of th	ar par - 610 Th		(b)(6),(b)(7) up with SA(C) and pr	ocess
(b)(6),(b)(7)(C) The thread below to the standard of the stan	has the status of the	equest that CPD Crim	e. e Soene personnel hook eft the other day after we	up with SA(C) and pr	ocess
(b)(6),(b)(7)(C) The thread below the newest external factor of the second control of the newest external factor of the new external factor of	has the status of the off today I would real hard drive for prices	equest that CPD Crim ints that the suspect I	e Scene personnel hook aft the other day after we	up with SA <u>(C)</u> and precleared the scene.	
(b)(6),(b)(7)(C) The thread below the newest external As you'll notice from	has the status of the off today I would real hard drive for prior the thread, the o	equest that CPD Crim ints that the suspect I	e Scene personnel hook aft the other day after we	up with SA(C) and pr	
(b)(6),(b)(7)(C) The thread below the newest external As you'll notice from	has the status of the off today I would real hard drive for prior the thread, the oup and downloading	equest that CPD Crim into that the suspect I operation is being sho ng data.	e Scene personnel hook aft the other day after we	up with SA <u>(C)</u> and precleared the scene.	
Subject: Fw: MIT (b)(6),(b)(7)(C) The thread below: As I am on a day of the newest external computer hooked in the computer hooked in	has the status of the off today I would real hard drive for prior the thread, the out and downloading	equest that CPD Crim ints that the suspect I	e Scene personnel hook aft the other day after we	up with SA <u>(C)</u> and precleared the scene.	
Subject: Fw: MIT (b)(6),(b)(7)(C) The thread below: As I am on a day of the newest external thread below: As you'll notice fro computer hooked:	has the status of the off today I would real hard drive for prior the thread, the oup and downloading phone number is	equest that CPD Crimints that the suspect I operation is being shing data. (b)(6),(b)(7)(C)	e Scene personnel hook aft the other day after we	up with SA(C) and procleared the scene. nue the investigation just not wi	
Subject: Fw: MIT (b)(6),(b)(7)(C) The thread below in the newest external thread below in the newest external thread by the newest external thread in the new external thread in thread in the new external thread in thread in the new external thread in thread	has the status of the off today I would real hard drive for prior the thread, the oup and downloadin phone number is	equest that CPD Crimints that the suspect I operation is being shing data. (b)(6),(b)(7)(C)	e Scene personnel hook eft the other day after we it down and we will conti	up with SA(C) and procleared the scene. nue the investigation just not with the investigation in the investigatio	
Subject: Fw: MIT (b)(6),(b)(7)(C) The thread below the newest external and the new	has the status of the off today I would real hard drive for prior the thread, the oup and downloading phone number is	equest that CPD Crimints that the suspect I operation is being shing data. (b)(6),(b)(7)(C)	e Scene personnel hook aft the other day after we	up with SA(C) and procleared the scene. nue the investigation just not with the investigation in the investigatio	
Subject: Fw: MIT (b)(6),(b)(7)(C) The thread below: As I am on a day of the newest external accompanies in the computer hooked (b)(6),(b)(7)(C) cell	has the status of the off today I would real hard drive for prior the thread, the oup and downloading phone number is [(b)(6),(b)(equest that CPD Crimints that the suspect I operation is being shing data. (b)(6),(b)(7)(C)	e Scene personnel hook eft the other day after we it down and we will conti	up with SA(C) and procleared the scene. nue the investigation just not with the investigation in the investigatio	
Subject: Fw: MIT (b)(6),(b)(7)(C) The thread below: As I am on a day of the newest external externa	has the status of the off today I would real hard drive for prior the thread, the oup and downloading phone number is [(b)(6),(b)(equest that CPD Crimints that the suspect I operation is being shing data. (b)(6),(b)(7)(C)	e Scene personnel hook eft the other day after we it down and we will conti	up with SA(C) and procleared the scene. nue the investigation just not with the investigation in the investigatio	
Subject: Fw: MIT (b)(6),(b)(7)(C) The thread below in the newest external thread below in the newest external thread below in the newest external thread in the new external thread in the new external thread in the new external thread in thread in the new external thread in the new external thread in thr	has the status of the off today I would real hard drive for prior the thread, the oup and downloading phone number is [(b)(6),(b)(equest that CPD Crimints that the suspect I operation is being shing data. (b)(6),(b)(7)(C)	e Scene personnel hook eft the other day after we it down and we will conti	up with SA(C) and procleared the scene. nue the investigation just not with the investigation in the investigatio	
Subject: Fw: MIT (b)(6),(b)(7)(C) The thread below: As I am on a day of the newest external externa	has the status of the off today I would real hard drive for prior and downloadin phone number is (b)(6),(b)(equest that CPD Crimints that the suspect I operation is being shing data. (b)(6),(b)(7)(C) (7)(C)	e Scene personnel hook eft the other day after we it down and we will conti	up with SA(C) and procleared the scene. nue the investigation just not with the investigation in the investigatio	
Subject: Fw: MIT (b)(6),(b)(7)(C) The thread below: As I am on a day of the newest external externa	has the status of the off today I would real hard drive for prior and downloadin phone number is (b)(6),(b)(1) (c) (c)	equest that CPD Crimints that the suspect I operation is being shing data. (b)(6),(b)(7)(C) (7)(C)	e Scene personnel hook eft the other day after we at down and we will conti and hook up with her ar	up with SA(C) and procleared the scene. nue the investigation just not with the investigation in the investigatio	
Subject: Fw: MIT (b)(6),(b)(7)(C) The thread below: As I am on a day of the newest external externa	has the status of the off today I would real hard drive for prior and downloadin phone number is (b)(6),(b)(1) (c) (c) (c) (d)	equest that CPD Crimints that the suspect I operation is being shing data. (b)(6),(b)(7)(C) (7)(C)	e Scene personnel hook eft the other day after we at down and we will continue and hook up with her ar	up with SA(C) and procleared the scene. nue the investigation just not with the investigation in	ith the
Subject: Fw: MIT (b)(6),(b)(7)(C) The thread below in the newest external the new external the	has the status of the off today i would real hard drive for prior the thread, the oup and downloading phone number is (b)(6),(b)(1) (c) (c) (c) (d)	quest that CPD Crimints that the suspect I operation is being shing data. (b)(6),(b)(7)(C) (7)(C) (6),(b)(7)(C)	e Scene personnel hook eft the other day after we at down and we will continue and hook up with her are the continue and the conti	up with SA(C) and procleared the scene. nue the investigation just not with the investigation in the investigation just not with the investigation just not with the investigation in the investigation	ith the
Subject: Fw: MIT (b)(6),(b)(7)(C) The thread below in the newest external section in the new external section	has the status of the off today i would real hard drive for prior the thread, the oup and downloadin phone number is you call (b)(6),(b)(1) (C) (SOS)	quest that CPD Crimints that the suspect I operation is being shing data. (b)(6),(b)(7)(C) (7)(C) (6),(b)(7)(C) (b)(6),(b)(7)(C) (c)(du:(b)(6),(b)(7)(C)	e Scene personnel hook eft the other day after we at down and we will continue and hook up with her ar	up with SA(C) and procleared the scene. nue the investigation just not with the investigation in the investigation just not with the investigation just not with the investigation in the investigation	ith the
Subject: Fw: MIT (b)(6),(b)(7)(C) The thread below in the newest external section in the new external section	has the status of the off today i would real hard drive for prior the thread, the oup and downloadin phone number is (b)(6),(b)(7)(C) (BOS)	quest that CPD Crimints that the suspect I operation is being shing data. (b)(6),(b)(7)(C) (7)(C) (6),(b)(7)(C)	e Scene personnel hook eft the other day after we at down and we will continue and hook up with her are the continue and the conti	up with SA(C) and procleared the scene. nue the investigation just not with the investigation in the investigation just not with the investigation just not with the investigation in the investigation	ith the

The open questions will be if we decide to take it offline, is this something I can do with instruction or will I need help? Also, do we want to have the new drive printed? (b)(6),(b)(7)(C) (h)(h)(h)(y)(c) ole Partick Cardwin Hi there. I have collected about 705 of network truffic to far with about 98% of which is the ISTOR journal downloads. I've done some initial checking of the capture and I don't see anything that identifies a command and control channel. I was just wondering what the next step is. Thank you (b)(8),(b)(7)(C) Natural & Infrastructure Services Information Services and Technology (IS&T) Massachusetts institute of Technology Room (6)(8)(6)(7) Cambridge, MA 02159 (D)(D)(D)(V)(C) (b)(0),(b) mit adu

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement samitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sander immediately and delete it.

Prom:		b)(6),(b)(7)(C)	_MIT,EDU>	•			
Sent:		Mednesday, January O	5 <u>, 2011 5:02</u>	PM			
To:	(b)(B),(b)	1011	5 (b)(8),(b)(7)(C)		
Ce (b)(8),(b)(7)(C		10				
Subject:	F	Packet Capture					
AM - 0		*				•	
Hi there,							
I have collected about	70G of netw	ork traffic so far with	about 98% i	of which is t	the JSTOR	journal do	wnloads. I've
some initial checking of	f the capture	e and I don't see anyti	hing that ide	intifies a co	mmand ar	nd control	channel. I wa
some initial checking of wondering what the n	f the capture	e and I don't see anyti	hing that ide	intifies a co	mmand ar	nd control	channel. I wa
some initial checking of wondering what the n	f the capture	e and I don't see enyt	hing that ide	intifies a co	mmand ar	nd control (channel. I wa
some inkini checking o wondering what the n Thank you	f the capture	and I don't see enyti	hing that ide	intifies a co	mmand ar	nd control	channel. I wa
some inkini checking o wondering what the n Thank you	f the capture	and I don't see anyti	hing that ide	intifies a co	mm and ar	nd control	channel. I wa
some inkini checking o wondering what the n Thank you	f the capture	and I don't see enyt	hing that ide	entifies a co	mmand ar	nd control	channel. I wa
some initial checking of wondering what the n Thank you 6),(b)(7)(C)	f the capture ext step is.	e and I don't see anyti	hing that ide	entifies a co	mm and ar	nd control	channei. I wa
some initial checking of wondering what the n Thank you (6),(b)(7)(C)	f the capture ext step is. twork & Infr	e and I don't see anyti estructure Services	hing that ide	mtifies a co	mmand ar	nd control	channel. I wa
some inkini checking o wondering what the n Thank you 6),(b)(7)(C) No Information Services a	f the capture ext step is. twork & Infr nd Technolog	e and I don't see anyti astructure Services By (IS&T)	hing that ide	mtifies a co	mm and ar	nd control	channel. I wa
some initial checking of wondering what the normality you (6),(b)(7)(C) Information Services e Manachusetts institut	f the capture ext step is. twork & Infr nd Technolog	e and I don't see anyti astructure Services By (IS&T)	hing that ide	mtifies a co	mmand ar	nd control	channei. I wa
some initial checking of wondering what the normalization for the	f the capture ext step is. twork & Infr nd Technolog e of Technolog	e and I don't see anyti astructure Services By (IS&T)	hing that ide	mtifies a co	mmand ar	nd control	channei. I wa
some initial checking of wondering what the normalism Services a Massachusetts institut Room (5/8)/6/7/	f the capture ext step is. twork & Infr nd Technolog e of Technolog	e and I don't see anyti astructure Services By (IS&T)	hing that ide	mtifies a co	mmand ar	nd control	channei. I wa